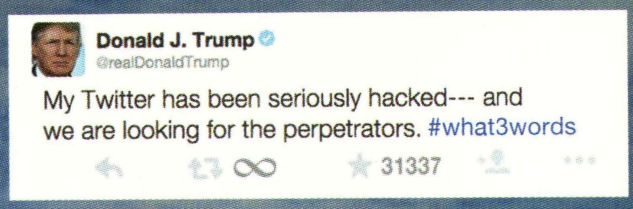
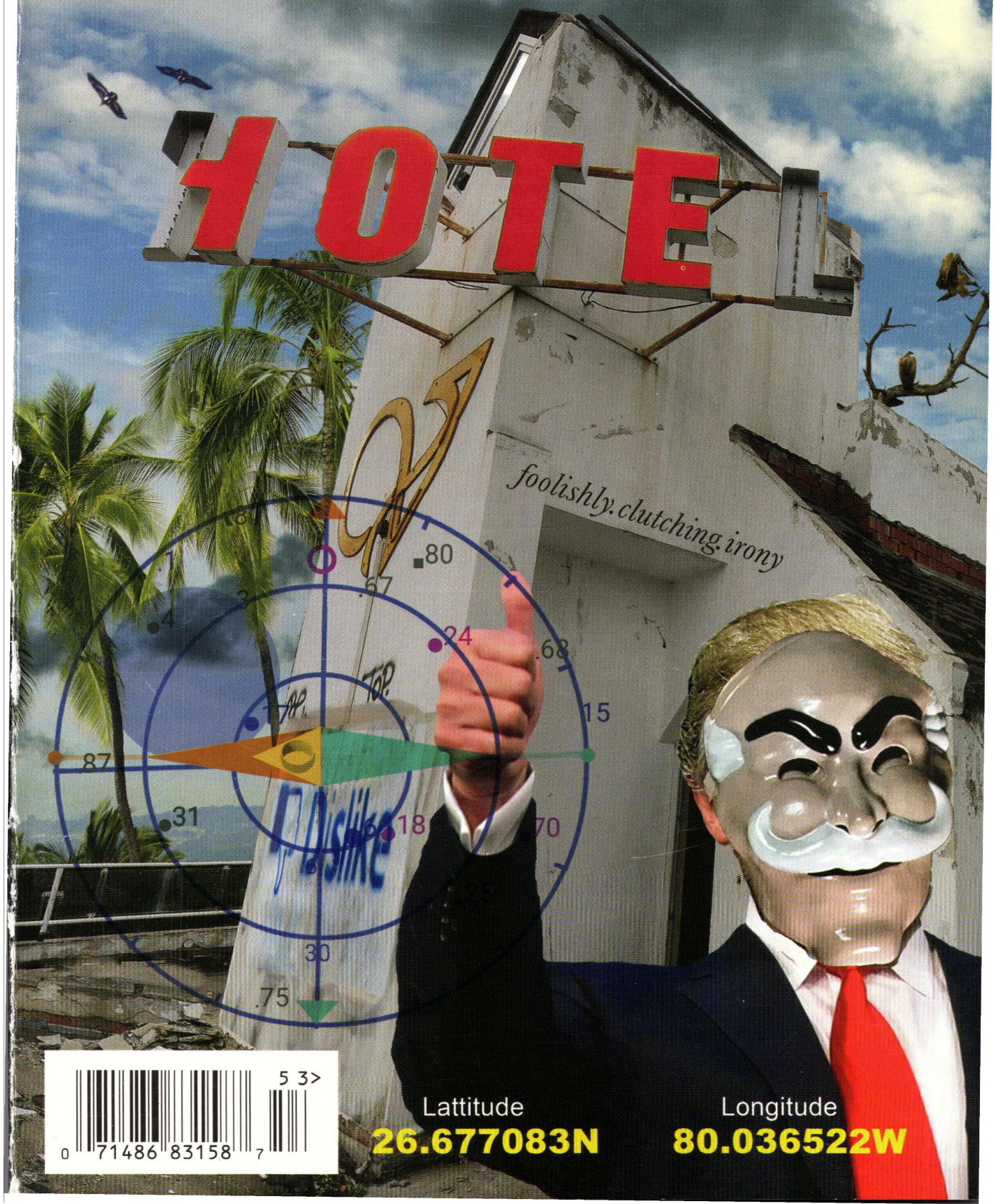
Volume Thirty-Two, Number Three
Autumn 2015, $6.95 US, $8.95 CAN

2600

The Hacker Quarterly


Donald J. Trump
@realDonaldTrump
My Twitter has been seriously hacked--- and we are looking for the perpetrators. #what3words
31337



5 3>
0 71486 83158 7

European Payphones

Croatia. A standard phone booth found in the small car-less village of Valun on the island of Cres.

Photo by Mandrappa Kurelek

Luxembourg. Found in the mountainous village of Vianden, this phone booth looks like it's attached to a mountain.

Photo by Mikel Shilling

Poland. Yet another small town booth found in Krynica. It's wheelchair accessible with no door, a ramp, and handlebars inside. A sticker says "Telefon Dwukierunkowy," which means "two-way phone" (you can make and receive calls here).

Photo by Dariusz Dziewialtowski-Gintowt

Greece. Yes, you guessed it - another small village with a payphone. This one is Plakias on the island of Crete, right by the water. There's some kind of connection between old, scenic villages and working payphones.

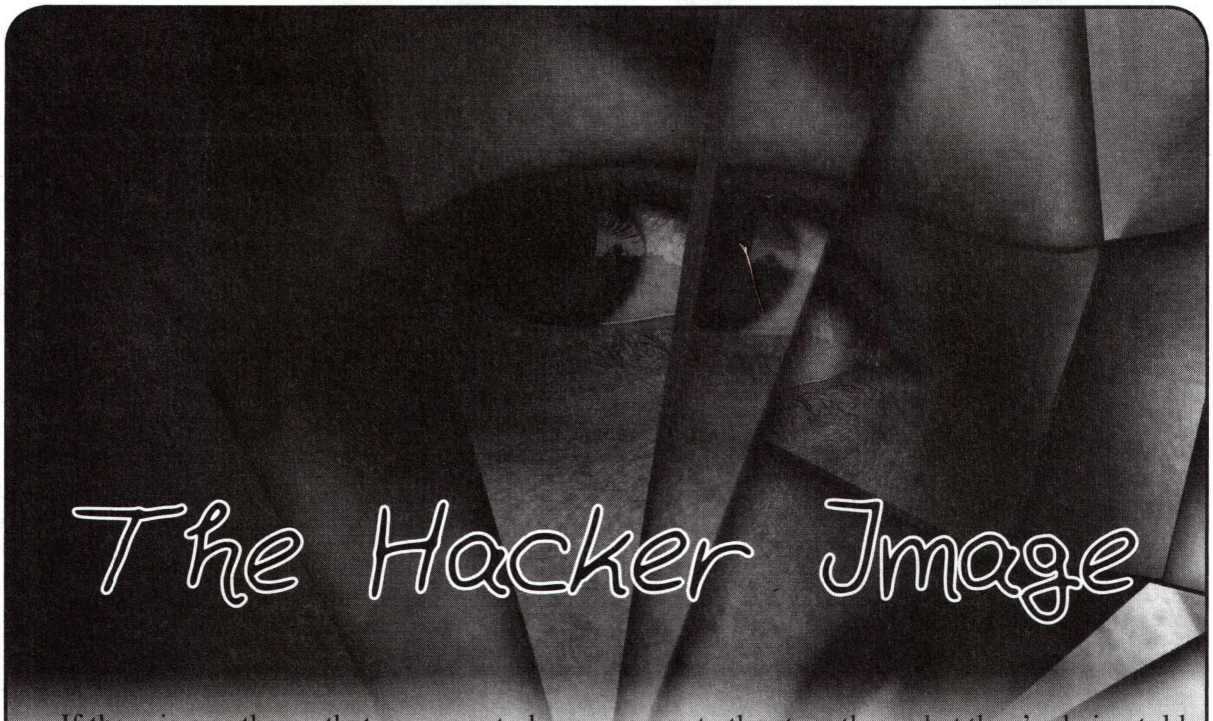
Photo by Mandrappa Kurelek

Got foreign payphone photos for us? Email them to **payphones@2600.com**. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)

PERCEPTIONS

The Hacker Image	4
A Primer on Home Automation (and How Easy It Can Be)	6
Dangerous Clouds	9
Unexpected Denial Of Service	11
A Convenient Method for Cloud Storage with Preserved Privacy	12
TELECOM INFORMER	13
Ashley Madison Military Sites	15
The Technology at QPDC	17
Open Source Repository Abuse	21
My Voice Is My Key	23
HACKER PERSPECTIVE	26
Fun with Billing Forms and International Debit Cards	29
Going Nuclear - A Tale of Revenge	30
Malware Attacks - Leave Those [Banks] Alone	32
LETTERS	34
Mr. Robot - A Ray of Light in a Very Dark World	48
Cruising the Wideband Spectrum	50
EFFECTING DIGITAL FREEDOM	52
The Dawn of the Crypto Age	54
Account Hack: Anyone Can Be a Victim	57
Fiction: The Stars Are Tomorrow	58
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

taking it to eleven



The Hacker Image

If there is one theme that we seem to have been locked into from the very beginning, it's that of preserving, correcting, and maintaining the image of hackers. To say it's a frustrating task would be a monumental understatement. But it's one that we should never give up on.

The media is by far the biggest culprit in sullying the name of hackers. They do this simply for their own benefit - to sell papers, get website views, achieve higher ratings. They need a demon and we happen to be it. Others base their perception on what they see in the media and it becomes an avalanche of misinformation and unwarranted fear. But there's one often forgotten fact that happens to be on our side. It isn't working.

Look at the villains you see portrayed in a normal half hour of fear mongering: killers, terrorists, rapists, and all of the assorted white collar criminals. For the most part, nobody aspires to be like any of these people. But while hackers are also injected into the mix as miscreants who cause great disruption and are capable of far more, so many people continue to want to *become* hackers. That's not exactly the kind of cause and effect you might expect from such a negative portrayal.

Why is this? Put simply, what hackers do is interesting and also extremely valuable. We maintain that hackers are, in fact, essential to a healthy society. Our image among the enlightened happens to be just fine. Anyone who doesn't automatically buy into the mass media portrayal likely already knows there's a lot more to the story than what they're being told. So we're far from alone in our perceptions.

But let's not underestimate the damage that such inaccurate portrayals can cause. Any individual suspected of being a hacker faces persecution in school, at home, and in the workplace, not to mention unwelcome attention from true criminals. The suspicion oftentimes never goes away. The mental effects this can have on a bright and impressionable individual cannot be emphasized enough. Sure, it's great that kids everywhere still want to be hackers. But if the hackers themselves are being treated like criminals and otherwise made miserable, what exactly are we gaining?

Like we said, we've been struggling with this from our very first days. And all that has really changed is the sheer *amount* of bullshit in the media that needs to be dispelled. Let's look at a bit of it from the present:

Hackers can take over airplanes. The jury is still out on the amount of access anyone could conceivably gain either as a passenger or as an interested party on the ground. One thing is for certain: a hacker will be the one to reveal this and share it with the world. And, if true, *anyone* would be able to take over a plane, including some very nasty people who know nothing of hackers. Who would you prefer to hear it from first?

Hackers can crash your car. If cars are actually being designed in such a moronic way that they can be controlled remotely, then you can bet the people who would *want* to

take over a vehicle would mostly be police, carjackers, terrorists, and angry spouses. Again, you will likely learn of this from a hacker because they will be the ones to figure it out. As for who will abuse it the most, that's really anyone's guess.

Hackers want to invade your privacy. The thing everyone seems to forget is that hackers are human beings, no more or less perfect than anyone else. It's certainly possible for a hacker to violate trust and cause mayhem, and that can be for a good cause or merely for personal gain. Something like the recent Ashley Madison data dump or last year's Sony incident doesn't necessarily have anything to do with hacking in the first place. If a master password was all that was needed, where is the hacking if that was simply found or revealed by a disgruntled employee? Once more, anyone could get this info with the right amount of access. And if a decent hacker was running their site, there likely would have been better safeguards in place from the start.

Education is key in correcting all of this or at least attempting to. Let's not ever accept negative connotations attached to the word "hacker." Let's not be intimidated into playing down our hacker connections. We've seen some hackerspaces do precisely that and stop using the word "hacker" to avoid scaring people, which is about as wrong an attitude as is imaginable. And creating new words to separate good from bad is worthless, as the values that mean so much to us are often seen as a threat to those in control and we wind up being labeled negatively with some new and absurd designation like "cracker" or "black hat." Only this time, the label has no positive interpretation in any way and we're all simply seen as criminals and not much else. Accepting these terms is a fast track towards the overall demonization of hackers and that hurts not only our community, but *anyone* interested in freedom and access.

Hackers have helped to build Apple, Google, and even the Internet. There's good and bad in all of that, but we maintain it would be a far more negative world had the skill of hackers not been appreciated and put to good use. Working for a giant corporation is not what makes a hacker "good," no more so than working against a government makes one "bad." It's far more complex than that and the media tends to want things to be as simple - and as scary - as possible. We don't have to play that game.

What we *can* do instead is continue teaching the world what hacking really means. It's about preserving privacy, revealing the truth, constantly testing security, figuring out better ways of doing things, and explaining how systems work to anyone who's interested. Preserving anonymity and protecting our identities using encryption are both basic values that hackers tend to believe in rather strongly. Interestingly, those at the forefront of the witch-hunt against the hacker world subscribe to neither. And that speaks volumes about motivation and goals.

Never be afraid to celebrate who you are as a hacker. But always be open to changing your perspective, your opinions, and your direction. That, after all, is how progress is made.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2015. Annual subscription price $27.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	28480	28906
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4020	4023
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	23492	23915
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	27512	27938
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	143	143
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	825	825
E. Total free distribution	968	968
F. Total distribution	28480	28906
G. Copies not distributed	0	0
H. Total	28480	28906
I. Percent Paid	97	97

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

A Primer on Home Automation (and How Easy It Can Be)

by Ilyke Maasterd

This article is based solely on my personal experience. I was recently very pleased to realize that "hardware tinkering" could be something even I could have fun with at home. I am usually more of a software guy. This is a story where one interesting thing simply led to another, and through which I learned many new things.

You may wish to read on more particularly if you have, yourself, a system similar to what I had before I started:

- one Onkyo AV receiver (audio and video amplifier with five HDMI inputs and an FM tuner) My particular receiver model could not handle DVI signals from the PC, however my TV model could. For best video playback, I acquired an HDMI signal splitter and connected to the receiver for sound, and to the TV for picture.
- one large television display
- one disc player
- one cable TV source, also serving as a PVR
- one PC capable of two distinct video outputs
- one LCD monitor for office computing at a nearby desk
- a few six-foot HDMI cables

Things can really kick off if you can afford or already have the following:

- one Harmony Ultimate Home from Logitech
- one Bluetooth-capable PC
- literally *any* IR-commanded appliance that is around (dehumidifier, portable heater, fan)
- Fancy: one set of speakers with a large bundle of speaker wires (or a Bluetooth alternative) to hear radio or a playlist of songs anywhere around the house
- Fancy: Wi-Fi thermostats to control room temperature and utility costs
- Fancy: Wi-Fi 120 VAC power adapters and extension cords to control lighting (or other)

The Genesis

The idea of pursuing home automation came to me when I realized that, as proud as I was to be able to "do anything" with my home theater system, it was always a little hassle to set up everything to get it working in different configurations. Well, if you are in this situation and follow through this article, you just may be able to consider yourself completely rid of that problem afterwards.

So I went out and decided to buy a Harmony Ultimate Home from Logitech. Not a product with a low price tag, but all I can say is that from my personal experience, I consider it well worth it. Truth be told, my real idea was to "buy it, figure out how to program it with Linux, and enjoy home automation," but I actually did not know much about Linux in the first place. I decided to buy the Logitech product at that point (nice decision). It is safe to say that this remote has clearly slowed my learning of Linux!

So the product comes mostly in three parts: an AC-powered repeater hub, an AC-powered charging cradle, and a battery-powered remote control. The remote control is quite enjoyable to use as it is ergonomic, the buttons work nicely, and the touchscreen display is pretty to look at and works very nicely.

The remote and hub communicate through radiofrequency (RF) and the hub then sprays the room with infrared (IR) codes to the appliances. For those unfamiliar, RF are radio waves that can go through walls and, quite obviously, do not require you to point the remote control at the device to be commanded; IR signals are different in that they are line-of-sight signals, which sometimes can reflect, and are the standard used in almost every wireless home product (disc player, cable TV, ceiling fans, etc.).

The remote setup could not be easier. First, you record your appliances with their make

and model numbers, as declared by the original manufacturer. Then, you program activities, which defines combination of devices, their setup, and the necessary sequences. That's it, you can enjoy life much better now with only that. With the app from Logitech and a Wi-Fi network, you can control your devices from a tablet and, literally, from the International Space Station if you can get there.

But it gets better. In this article, I will totally skip over the Logitech product details and input methods as they are quite easy to learn. I will only describe the appliances and activities I have come up with on my own as well as attempt to show how interesting things can become. I expect these descriptions will contain enough details for anyone to experiment easily on their own. I also assume that your different appliances are all already connected properly.

Please do try this at home.

The Basics

The first rule is: if you can produce the desired changes through the remote, you can execute it with Harmony. Begin by programming a few appliances and then come back to reading this. Start with: TV, cable, disc player, and finally, amplifier.

As I said, that step should have been easy enough. You now have a few different devices programmed in and with a single RF remote, you can control them from way farther in the house. You do not have to bother anymore to get your arm out from under a blanket to pause, rewind, or whatever.

Programming activities is the next step. Again, with the default interface, all of the different scenarios you use regularly will be easy enough to configure. Select the devices involved, specify the output and input channels of each for the activity, and voilà, you are done. You can now, after a long day at work, pick up the remote and press a *single* button on it to enjoy the ongoing live hockey game of your favorite team. If the game turns sour and you change your mind, another *single* key press will reorganize everything to play the movie you left in the middle of the previous night.

More Fun

The second rule is: if you can script commands on a PC that is Bluetooth-capable, you can execute them with Harmony (in conjunction with other tools).

Here I will avoid the subjects of how scripting through batch files (.BAT) is performed, as well as how Bluetooth pairing is performed. I suggest anyone not familiar with these topics do a quick web search, and read forum answers. What I will describe, however, is how to take advantage of the fact that the Harmony is Bluetooth-capable.

I had never taken advantage of Bluetooth on any device, ever, until I bought the Harmony product. Reading up on it on the WWW, I came across a great little software called PS3BluMote.[1] It is there that I learned that the PlayStation PS3 is one of the rare gaming consoles to support Bluetooth, and somebody had already figured out a way to take advantage of the Harmony's compatibility. While I do not actually own a PS3 console myself, PS3BluMote lets me take advantage of Harmony to basically send commands from my Bluetooth-capable PC. I will describe PS3BluMote in a little more detail later. First, a real-life example may prove useful to illustrate the convenience one can enjoy.

I had the issue that my amplifier would not display properly the video portion of the DVI-over-HDMI signal coming from my PC while the sound transmitted fine. Through my amplifier, the video came out full of artifacts and colors were miscoded. Watching a movie this way was not acceptable. The DVI input of my TV being perfectly compatible, I elected to display video through the TV input, and playback audio (in 5.1 surround) by selecting the GAME input of the amplifier. I was thus able to watch a movie with good picture and good sound. This setup requires using an externally-powered HDMI signal splitter to duplicate the PC source signals.

The problem was that in Windows, sound is not directed to all outputs simultaneously; only one audio output device can be active at a time. So when I am in normal office configuration, the PC uses a set of small PC speakers to play sounds and music. One must direct the audio output to the PC's HDMI jack through a small labyrinth of Windows settings. This

operation is only meant to be a manual one for security purposes and over time it becomes a bit tedious, but mostly boring, to change the PC's audio output device.

Then comes a lifesaver, another great little program called NirCmd.[2] Based on the NirCmd instruction set, I produced short batch files that can switch the audio output device of my PC without mouse interaction (do not ask me how that is done by NirCmd - it just works). So I created on my desktop a first shortcut that points at a script called "Audio to speakers.BAT" and another shortcut that points at a script called "Audio to amplifier.BAT." All these scripts contain are two NirCmd commands: the first line changes the audio device and the second line speaks the description of the device out loud (through voice synthesis).

Now it's time to take advantage of the fact that Harmony supports controlling PS3 consoles over Bluetooth. By setting it up to connect to a fake console receiver through PS3BluMote, you can easily execute any script of your liking on the PC. The magic is simply done by creating shortcuts to your scripts on your Windows desktop, and by assigning keyboard shortcuts to them (e.g. CTRL-ALT-0). Then you simply need to configure PS3BluMote to react to a specific button (e.g. Channel Down) by producing the desired key presses through to Windows by means similar to the SendKeys method. In my case, Blue commands the PC's audio output to the cinema system. Yellow reverts the PC's audio output to the small speakers.

Once these scripts execute reliably, it becomes trivial to introduce them within existing Harmony activities such as "Watch movie from disc" and "Watch movie from PC."

The Fancy List

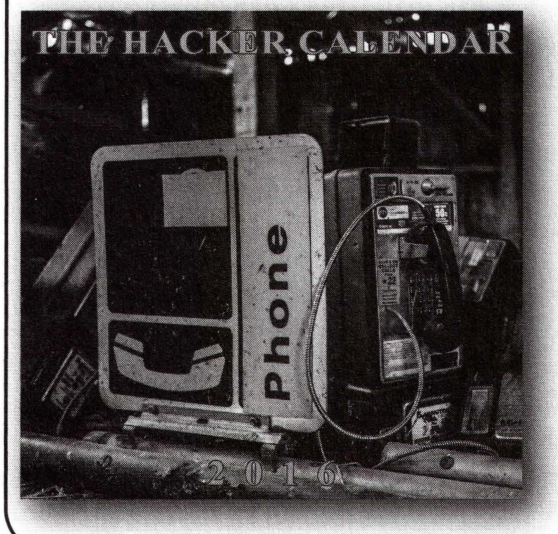
These are things I have just not yet gotten around to doing and have not yet coughed up the money for, but they are all things that I am looking forward to implementing some day. My very next step will be to kill the lights when setting up to watch a movie by using home automation power adapter(s).

I hope you enjoyed this guide as much as I enjoyed constantly improving my activities and associated sequencing. I would really love to hear of more unusual ideas to take better advantage of this hardware; please share your experiences in these pages!

1. https://github.com/Ben-Barron/PS3BluMote/blob/master/README
2. http://www.nirsoft.net/utils/nircmd.html

IMPORTANT NEWS:

2016 CALENDARS



The 2016 Hacker Calendar is out!

Each month features a 12"x12" glossy photo of a public telephone from somewhere on the planet, and nearly every day marks something significant in the hacker world.

Get yours today at store.2600.com!

DANGEROUS CLOUDS

by Donald Blake

Using a cloud-based system is all the rave these days. It's efficient, fast, and easy to use. You really can't live in today's society without using a cloud-based system to store your data. With all the commercial cloud-based systems out there, one has to wonder who's got more data - the government or commercial enterprises.

From the various government agencies I know, they collect some pretty valuable information. I know they have my address, driver's license, tax information, employer information, phone number, Social Security number, passport, and legal history. They also collect various bits of information about me every year or every couple of years, but this is pretty much what they have. They may have other data on me from some classified operation. But seriously, even if they do, the list of data sources above paints a pretty good picture of me anyway. Besides, how big can their database really be and how much do they care about me? I'm just a regular Joe trying to keep a job, pay my bills, and find girls. I'd be flattered if *a person* ever wanted to know everything there was to know about little old me.

I'm not completely out of luck because there are computer systems out there that *do* want to know me - down to the smallest detail. Cell phones are really just a human tracking system. Cell phone companies track your every move and can locate your phone at any time anywhere as long as it's on. They know where the hell you are at every minute of the day! Cell phone companies really do care how you use your phone because there's a dollar value attached to it. The ability to track you makes it so they can provide you with better service and they can also tell you where you go over a course of time. They can also sell this information to other companies that could use this data as well.

I'm still waiting for the day businesses start caring about IP addresses that walk in their door. That would give them so much power. That would tell them how many people come into their stores just to browse and how many actually bought something. They would also know how long their customers stayed in their store. If they also talked to the navigation companies, they would know where their customers came from and went to after visiting their store. With that information, they could better serve their customers. They would basically be able to get for a physical store the kind of data a website gets from people who visit the site.

When was the last time you set foot into your financial institution? Has it been a while since you last talked to a teller at your bank? If the answer is yes, then you're not alone. Most people don't go to their financial institution anymore. They can get everything they need online. Nice and convenient, isn't it? Everything is fed into a computer which is then stored in a database somewhere. If you were a financial institution, wouldn't it be cool if you knew what your clients were buying? Then you could use that information to sell products to your clients. When they go shopping for a car, you could analyze their financial situation and tell them if the car they were thinking of buying was something they could afford. Since you have the same type of data on other people, you could also tell them if it was a good deal or not because you would know how much other people paid for the same car. Then you could offer them a nice loan for it too! With your members' permission, you could also make this information available for others' use for other reasons.

We can be whoever we want to be. Let's be someone who's interested in stocks. If we could tap into financial institutions and find out what people were buying and from whom, then we could tell which companies were going to be profitable or not. Why care about earnings? We know exactly who's profitable and who's not because we're watching what people buy! Forget about government reports that come out every so often We can tell how well the economy is doing and our information is in real time!

This isn't that difficult to do. All you need to do is analyze the financial institutions database and look for the merchant's name, and then note what the person bought and from whom. This could be broken out into reports since storage and bandwidth is cheap. The cost of computers, networking, and manpower to maintain all of this is expensive; maybe the financial institution was nice enough to outsource all of their computer operations to another company like Member Driven Technologies. Assuming that the outsourced company has multiple clients, they could have trillions of dollars located on their servers! Feel free to use your imagination with what else you could do if you got a hold of that data!

Humans are social creatures. If we don't talk to other people, we develop problems. What you put online has an effect on your social status. We want to show our friends what we are doing and they want to know what our friends are doing. We post pictures of our families as well as events that we attend online. It sure as hell beats printing photos and putting them in an envelope with a note to all of our friends and family talking about the event. It's so much easier to put them on a social media site and share. However, by doing this, we give away a lot of personal information. The social media company uses this data to make money. The media will also use it to identify you and help them with their story if you do something that is newsworthy.

Everything is connected to the Internet these days and more and more devices are coming online every day. Practically everything you use that has a computer in it can and will send data to some company database somewhere. Companies use this data to better serve their customers and also to make their software better. It also makes sense to put stuff on their servers that is accessible anywhere because the user can access their data wherever they go and from whatever device they want. Couple that with a terms of service agreement that flirts with the lines "Any data you send us we can use and sell" and bury it in the small print and then the company is golden! They now have a very good reason to make your data useful, searchable, and marketable! They now know what advertising to send you and what things you're likely to buy because they've analyzed your data - which you were so nice to give them for *free!* It also makes sense for them to invest in these systems because your data is driving their business. The more data you give them, the more valuable their systems become and the larger these cloud-based systems become.

People are so worried about the government tracking people. You probably are in some classified government database, but seriously, how big could it be? For the government to track you, they have to have a budget and it has to be approved by a group of politicians. It's a government run operation, so we know that whatever that database looks like, it's not going to be done efficiently. When they go about building this database, they'll have to go through contractors to get the parts, which will probably lead to a cost overrun. Also, the people who work on it aren't going to be the best because government employees do not get paid as much as employees of private companies. Not to mention someone somewhere knows about this system and, depending on the country's mood and politics, it could be declassified.

On the other hand, companies that offer cloud-based solutions have way more data than any government could ever get! They also want to make their systems bigger and better, because if they do that, then that means they make more money off of all of the data they can get. It pays for them to make these systems as efficient as possible and as high quality as possible. Not to mention that some of these cloud-based systems have contracted with the government and hold your data on their systems for the government! Considering the data I have in some of these cloud-based systems, the government really is the small fish in the lake. It's really funny to me when I read a story in the news about companies that run cloud-based systems telling the government to not collect data!

I really wish someone knew everything about me other than a computer.

Thanks for reading.

References

Member Driven Technologies: `https://www.mdtmi.com/`

Shout out to Violet.

UNEXPECTED DENIAL OF SERVICE

by J. Savidan

I work as an ERP consultant for a big IT company in France (this precision should explain my relative lack of fluency in English), and it is not particularly fun on a daily basis.

But a few days ago, something a little more spicy happened: I had to install a patch in production, nothing really difficult or dangerous.

As part of the procedure, my customer wanted a proof that only the impacted programs were installed. I had that requirement on the previous installation also, so a few weeks ago I wrote a utility program that scans two environments and yields the differences between them.

To check the version and the signature of one program in particular, all we have to do is to use a web form that checks this for you after being given the name of the program.

To do that for almost 9000 programs, I needed a way to automate this in one way or another.

My solution was to write a Java program that opens an http connection to the address of the lookup form, providing the name of the program to look up in the http request. Then all I needed was to do that for every line of a file containing the list of all programs, and I had a super fast web bot.

I added a parameter corresponding to the time the program has to wait before issuing the next request.

The code is very simple, and can be shortened to something like this:

```
FileReader fr= newFile
➥Reader(newFile(programs
➥Listing));
BufferedReader br =
➥ newBufferedReader(fr);
while(br.ready()) {
  String prg= br.readLine().
➥trim();
  URL finalURL= newURL("www.a
➥-server.com/findClass?port=
➥6100&p1="+prg);
  URLConnection conn= final
➥URL.openConnection();
  BufferedReader in= new
➥BufferedReader(new Input
➥StreamReader(conn.getInput
➥Stream()));

...

Thread.sleep(Integer.parse
➥Int(wait));
}
```

The rest of the code reads the buffer to do some DOM parsing to retrieve what the web form would produce on screen.

On D-Day, I launched my scan with a 500 millisecond delay. Strangely, an hour after this, the production became unstable.

The IT operations team suspected my patch to be the troublemaker, but none of the issues reported could be logically caused by a mere software patch.

I was the only one to suspect my analysis tool, and I began to check the log files for some hint.

It was simple to figure out: the application container was trying to create a new JVM (for load balancing) using a servlet, and an http exception was occurring.

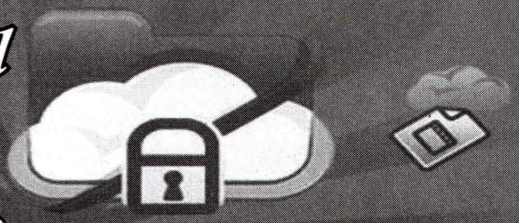
That was just in the middle of my long scan, and I realized that my tool was flooding the server with http requests, causing other requests to timeout, and in particular one with a URL ending with "/addJVM".

That was an involuntary denial of service, and it was quite efficient, judging by the raising of temperature on the client's side!

What's most funny is that they have an expensive supervision tool which triggers an alarm as soon as you act on a JVM, even if the action is a necessary maintenance action - but it's not able to detect an unusual count of hits on the web port....

Of course, they still don't know the truth. That's the price you pay when you don't know how to read a log file....

A Convenient Method for Cloud Storage with Preserved Privacy



by Alva Ray

I have seen mentions of this on the web, but not in *2600,* and since I think it can serve many readers of these pages well, I decided to submit an article on the subject.

There are many good and convenient cloud services out there for storing files. In light, however, of recent events regarding NSA mass surveillance of Internet traffic, once again the question of privacy has made it into our collective conscience. This article describes a simple mechanism for storing sensitive data on any such service in a way that makes it unavailable to prying eyes - most importantly from the service provider, should they decide to give the data to a third party. The answer, as always, is client-side encryption, since we cannot and should not trust a service that claims to encrypt your data in a way that makes it off-limits to them. You know, trust no one. But manual encryption and decryption of data before storing it online can be a hassle and we want to remove as many steps as possible.

I will use the popular Dropbox service as an example, but the described method, of course, applies to any similar service. I will also assume Mac OS X only because that's what I use myself, but the same method should be available to all operating systems with some sort of support for creating and encrypting disk images.

First off, there is a special "sparse" disk image format which means that even though the mounted volume can have any size, it will only occupy disk space according to how much data the created disk holds, plus a bit of overhead. For example, I can create a one gigabyte sparse disk image, but it will initially only use 40 megabytes of space and then grow as I add files to it. The built-in Disk Utility application in OS X can create such images, and also encrypt them using 256-bit AES and a password you supply. All of this can be configured in the dialog that pops up when clicking "New Image." Be sure to set the options for disk size, encryption, and the image format "sparse disk image." The resulting file is a secure disk that you can happily put in Dropbox to be synched, and share it with others who have the password.

Once the disk image is in Dropbox, you continue using it by just double-clicking the image to mount it, which will ask for your password. For even higher security, don't opt to save the password in your keychain. Now, copy the files you want to protect to the mounted disk and eject it when you are done. The disk image will immediately sync to Dropbox, but none of the data on it will ever have left your computer unencrypted. Sitting on the Dropbox servers will be a binary blob of data that no one without the password can open, due to the nature of strong encryption. The disk image will take up as little space as possible on your computer and, if you want more space on it later, the Disk Utility tool can resize it dynamically without altering the content.

What we have done here is to use built-in tools of the operating system to create a secure storage, while leveraging the general usefulness of a service like Dropbox. You will obviously not be able to browse the files on this disk through the Dropbox web interface or anything other than your computer, but in that specific setting it is great, especially since it's super easy to share the disk with anyone on a similar setup.

To sum it up: Don't trust cloud services no matter what privacy claims they make. Always rely on client-side encryption rather than server-side. Make use of the good services out there but bend them to serve your own purposes. In other words, rely on the hacker mentality and maintain control over your own data.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! This summer has brought surprisingly little travel to far-flung corners of the world. My employer has kept me in a management role, but I'm now working on a lot of mobile technologies. This is really where the action is. Very capable smartphones are selling for as little as $50 nowadays, and the rate of POTS disconnections and port-outs is only accelerating. However, the company is actually holding its own in broadband. This is being done through deployment of fiber-to-the-node, a topic for a future column. Broadband, however, is an unregulated service, like wireless. The days of PUC-regulated POTS lines, however, are clearly numbered. In the past year, things have changed very rapidly - from consumer expectations about reliability to the plummeting price of wireless voice service (which, as of this writing, is actually free from ringplus.net, a Sprint MVNO) to the way that people purchase handsets, choose carriers, and pay for service (contracts have been all but eliminated thanks to T-Mobile's competitive moves).

And then there's the inside of prisons. Remember the kid a few years ago who was dealing drugs from the payphone outside the Central Office? He called me the other day from prison. From his cell phone. And he made it quite clear that he wasn't pleased with my "service monitoring" that led to his current residential arrangement. I was a little taken aback, but not surprised. While federal prisons have somewhat kept pace with the evolution of technology by allowing prisoners access to limited e-mail technology, no prisons outright allow unfettered access to wireless phones. This hasn't stopped the proliferation of them inside prisons, though. It's actually a huge problem because a smartphone in the hands of an imprisoned and violent gang leader, for example, could be easily used to continue running a criminal organization from "inside." Or to harass me, for that matter. More commonly, though, prisoners use mobile phones to keep in touch with friends and family, and they have no criminal intent. They simply cannot afford to pay the extremely high prices charged by Global Tel*Link and other prison phone providers. And there is a matter of both safety and convenience; prisons seldom provide enough phones for inmate use and there is often violent confrontation over access to the few phones available.

Cell phones are also a lucrative source of income for corrupt prison guards, who are paid relatively low salaries. A simple TracFone can command up to $300 in prison. This is as equally profitable a revenue stream for guards as drugs are, but with less risk. Guards caught smuggling cell phones might lose their job, but are not subject to prosecution for a drug felony. Additionally, the demand in prison is higher than for drugs, and the safety risk to guards by an inmate with a mobile phone is perceived to be less than that of an inmate high on drugs (or, even more dangerously, alcohol). What's more, phones are periodically confiscated, often by the very same guard who sold them to a prisoner! This leads to a perpetual income stream. Sometimes seized contraband phones are even resold to other prisoners. In my view, it's somewhat ironic that corrupt guards have become the primary competition for the corrupt kickbacks paid to the prison system itself by operators such as Global Tel*Link.

Guards are the primary source of mobile phones in prisons, but they're sometimes smuggled in via other means. One prison in Russia discovered a cat that was wearing a vest with pockets full of mobile phones. It was enticed by prisoners to slip through the fence in exchange for food. Another prison had to install nets above its prison yard because of a number of incidents in which mobile phones were delivered by drone. In France, a truck was discovered with a false bottom and, rather than weapons or drugs, the contraband was - yep, you guessed it - mobile phones.

Smuggled mobile phones have been a serious problem for prison authorities for some time. In 2007, *An Omar Broadway Film* was clandestinely shot in the Northern State Prison in New Jersey. Contraband phones are prominently featured. Prisoners using mobile phones is such a common problem that Facebook even has a procedure for prison authorities to request the removal of Facebook accounts corresponding to users who are in prison (Facebook doesn't allow prisoners to use the service). It's also common to find videos on YouTube shot from prison; they show everything from the mundane details of everyday prison life to rap battles. And obviously, this is just the tip of the iceberg. It doesn't take the intelligence level of a hacker to know that you should probably keep a low online profile if you're in possession of a contraband mobile phone. So now, we're starting to see some high-tech and low-tech solutions to combat the problem.

In many countries, there is a fairly blunt instrument that is employed to combat the issue: jammers. Wardens in the U.S. have pushed the FCC for years to allow this in prisons as well, but the FCC unequivocally bans jammers in nearly all circumstances (the Secret Service reportedly has an exemption from this

ban for purposes of protecting the President's motorcade). The CTIA, a lobbying group for mobile phone companies, strongly supports the ban and opposes all use of jammers. This is, in my view, the right call; it's not reasonable for neighbors of a prison to be impacted by measures intended to prevent prison contraband. After all, a prison's neighbors aren't actually in prison themselves! So wardens have mostly resorted to low-tech measures: searches.

It is possible to train dogs to find mobile phones, and some prisons have done so. However, dogs are trained to smell electronics, not mobile phones, and a lot of electronics are actually allowed in prison. To a dog's nose, portable music players are nearly indistinguishable from mobile phones, and almost every inmate has a portable music player. So, dogs are really only effective at a prison's perimeter. They can help to find a stash of mobile phones secreted away in a hidden vehicle compartment, but they're all but useless inside a prison.

Prisons can also - in theory - hunt down unauthorized mobile phones using RF gear. After all, mobile phones broadcast within narrowly defined frequency ranges so, at least in theory, it should be possible to detect them. In fact, it's considerably more difficult. Prisons are made out of concrete and steel. This means radio signals reflect all over the place. Inmates live in very close quarters, and a very large number of them have mobile phones, creating a fairly massive amount of activity. What's more, there are a lot of *authorized* mobile devices inside prisons. Guards in many facilities, for example, are allowed to use their personal mobile phones in designated areas. Some prison doctors are allowed to use portable hotspots or personal mobile devices to look up medical information. The list goes on. Prisons using RF gear to find mobile phones have almost the same results as prisons conducting random searches.

In California, however, the state prison system may have discovered a method that works. In partnership with a mobile carrier (such as my employer), a special cell tower is installed within the prison walls. It essentially functions as a repeater that filters by IMEI or ESN. Here's how it works: authorized devices (along with the devices of complaining neighbors) are added to a whitelist. Every other device is blocked from accessing the mobile network, and an intercept message is played explaining how authorized users (e.g. people not in prison) can resolve the situation. Text messages and data services are also blocked. Such systems are blandly called "managed access solutions" and operate very similarly to Stingray devices used by law enforcement. However, these devices actively interfere with traffic rather than passively monitoring it. Sound good so far? There is a dark side. The largest provider of "managed access solutions" is a company called Securus, which provides inmate calling services at inflated prices (with requisite kickbacks to prisons). Obviously, their motive for being in the business is to protect prison phone revenues. Another company, meshDETECT, also provides these devices. However, their systems are more pragmatic; they can be configured to allow inmates to use cell phones, but ensure that they are subject to the same monitoring (and naturally, billing) as any other call made from a prison phone.

It's obvious that the current situation, where inmates have virtually unlimited access to mobile phones, is untenable. Most people don't belong in prison, but some inmates actually do belong there and have committed serious violent crimes. These offenders in particular shouldn't be allowed the relatively unfettered ability to continue directing criminal enterprises from behind bars. On the other hand, the vast majority of inmates with mobile phones just want to stay in touch with their family and significant others, and they don't want to bankrupt these people doing so. They don't actually present a threat. The technology exists to allow inmates access to mobile phones, but for this access to be monitored. As mentioned, it's called Stingray, and this is a technology that is not only widely used in criminal investigations, but it's already FCC approved. I think a reasonable compromise is to employ a Stingray inside all prisons, play a message indicating that all calls are monitored, and allow inmate handsets to be registered. However, mobile carriers should continue to provide the service at normal (not inflated) rates. Allowing greater access to (monitored) e-mail services hasn't resulted in any significant problems in federal prisons, so expansion of (monitored) access to mobile phones shouldn't result in significant problems either.

And with that, it's time to bring this installment to a close.

References

http://prisoncellphones.com/ - Lots of information about meshDETECT, a managed access solution.

http://gcn.com/articles/2013/09/➥05/prison-cell-phones.aspx - Good roundup article of managed access solutions from GCN.

http://gcn.com/articles/2013/09/➥06/managed-cell-access-prison-➥side.aspx - GCN article on the technical complexity of correctly deploying managed access solutions.

https://www.fcc.gov/document/➥contraband-wireless-device-nprm - FCC notice of proposed rulemaking for contraband cell phones. The essence of this is allowing managed access, but disallowing jammers within prison walls.

https://securustech.net/phone-➥services - Securus provides managed access solutions, but they appear to do this primarily to protect revenue from inflated prison calling rates.

http://www.ctia.org/policy-➥initiatives/policy-topics/contraband-cellphones-in-prisons - CTIA policy paper on why jammers should not be allowed in prisons.

https://youtu.be/ewSAoASIY4s - News article highlighting California prison efforts to keep cell phones out.

https://www.youtube.com/watch?v=➥EBIt0rMBVqU - Video roundup of camera phone shots sent from inside prison. A good look at prison life.

ASHLEY MADISON MILITARY SITES

We extracted all of the .mil domains that were listed in the recently leaked Ashley Madison files. None of these are verified since anyone could have entered any info without verification. But there are likely many valid military domains revealed here. So much for secrecy.

12mcd.usmc.mil
13meufwd.usmc.mil
1fssg.usmc.mil
1mardiv.usmc.mil
1maw.usmc.mil
1mawmag12.usmc.mil
1stiocmd.army.mil
22meu.usmc.mil
29palms.usmc.mil
2fssg.usmc.mil
2mardiv.usmc.mil
2mawbft.usmc.mil
2mawcp.usmc.mil
2mawnr.usmc.mil
3div.usmc.mil
3fssg.usmc.mil
3maw.mil
3maw.usmc.mil
3mawcpe.usmc.mil
3mawcpen.usmc.mil
3mawyuma.usmc.mil
4bct10mtn.army.mil
6mcd.usmc.mil
8mcd.usmc.mil
aaron.d.maxim.mil
aaron.h.baugher.mil
abss3.wpafb.af.mil
adab.centaf.af.mil
adam.g.koroll.mil
adder.arfor.army.mil
adrian.b.nettles.mil
af.mil
afg.usmc.mil
afghan.swa.army.mil
afghan.swa.mil
afip.osd.mil
afncr.af.mil
africom.mil
afspc.af.mil
ahqb.soc.mil
airstasavannah.uscg.mil
airtermnorva.navy.mil
ake5.navy.mil
ake8.navy.mil
ako.army.mil
ako.mil
albert.j.jacquot.mil
albirm.af.mil
albuquerque.smil.mil
alecarvalho.mil
alex.j.scott.mil
alexandre.mil
altus.af.mil
alvarado.a.ruiz.mil
amed.army.mil
amedd.army.mil
ammon.s.benedict.mil
ampla.mil
andersen.af.mil
andrew.d.messick.mil
andrew.l.bosanquet.mil
andrew.s.keith2.mil
andrews.af.mil
andrey.d.williams.mil
ang.af.mil
anthony.l.brown12.mil
antietam.navy.mil
antmobile.uscg.mil
antonio.camberos.mil
antonio.d.mcniel3.mil
anzio.navy.mil
aol.mil
apg.army.mil
apolo.mil
ar-usacapoc.soc..mil
arc.mda.mil
arcent.army.mil
arcent.mil
ardec.mil
arftsm.ang.af.mil
arifjan.arcent.army.mil
arl.army.mil
arleighburke.navy.mil
army.army.mil
army.mil
army.pentagon.mil
army.us.mil
arnold.af.mil
as39.navy.mil
as40.navy.mil
asclearwater.uscg.mil
asgastj.mil
ashland.navy.mil
asland.usmc.mil
ast.uscg.mil
atgl.navy.mil
auab.centaf.af.mil
aus.army.mil
austin.navy.mil
austin.r.bray.mil
autec.navy.mil
avenger.navy.mil
avonpark.macdill.af.mil
avy.mil
axwell.mil
az.ngb.army.mil
balad.iraq.centcom.mil
ballston.uscg.mil
bamrj.mar.mil
barksdale.af.mil
barry.navy.mil
bartolome.mil
bataan.navy.mil
beale.af.mil
beaufort.usmc.mil
belle.mil
beltran.mil
belvoir.army.mil
benfold.navy.mil
benjamin.c.corbett.mil
benjamin.j.weddle.mil
benning.army.mil
bernard.b.shields.mil
bgomez.mil
bic.usmc.mil
blab.accent.af.mil
blab.afcent.af.mil
bliss.army.mil
bloch.nrl.navy.mil
blue-ridge.navy.mil
bonhomme-richard.usmc.mil
bonhomme.richard.navy.mil
boone.navy.mil
borrego.mil
boxer.navy.mil
brad.a.joseph.mil
bradley.e.friend.mil
bradley.navy.mil
branden.d.davenport.mil
brent.w.kieran.mil
brian.g.crawford4.mil
brian.t.covert.mil
bricktop.mil
bruc.mil
bruno.mil
bryan.r.morrow4.mil
bulkeley.navy.mil
bunker-hill.navy.mil
byron.j.roberts.mil
ca.ngb.army.mil
cable.navy.mil
cachan.ang.af.mil
cafres.ang.af.mil
cannon.af.mil
cannon.afa.mil
cara.mil
carney.navy.mil
carswell.af.mil
carter-hall.navy.mil
casey.d.jones32.mil
catia.silva.mil
catia.siva.mil
cb.eb.mil
cbn72.navy.mil
ccad.army.mil
ccsg3.navy.mil
cds14.navy.mil
cds2.navy.mil
cen.amedd.army.mil
centcom.mil
cg-66.navy.mil
cg52.navy.mil
cg53.navy.mil
cg54.navy.mil
cg55.navy.mil
cg56.navy.mil
cg57.navy.mil
cg58.navy.mil
cg59.navy.mil
cg60.navy.mil
cg61.navy.mil
cg62.navy.mil
cg63.navy.mil
cg64.navy.mil
cg65.navy.mil
cg66.navy.mil
cg67.navy.mil
cg68.navy.mil
cg69.navy.mil
cg70.navy.mil
cg71.navy.mil
cg72.navy.mil
cg73.navy.mil
cgcbear.uscg.mil
cgcdiligence.uscg.mil
ch.mil
chafee.navy.mil
charleston.af.mil
cherrypoint.usmc.mil
cheyennemountain.af.mil
chief.navy.mil
choco.mil
christopher.j.hill89.mil
christopher.l.barreto
➥.mil
christopher.m.melton3
➥.mil
christopher.m.powell2
➥.mil
christopher.r.johnson
➥.mil
churchill.navy.mil
civ.mail.mil
cjfksg.navy.mil
cleveland.navy.mil
clifford.g.kendall.mil
cn75.nay.mil
cnet.navy.mil
cnfk.navy.mil
cnrc.navy.mil
cobuck.ang.af.mil
cole.navy.mil
colter.c.brown.mil
columbus.af.mil
columbus.navy.mil
comdt.uscg.mil
conus.army.mil
conus.mil
conus.us.army.mil
cook.navy.mil
cory.d.belvin.mil
cpen.med.navy.mil
cpr1.navy.mil
cpr3.navy.mil
crommelin.navy.mil
cssemnf-wiraq.usmc.mil
ctf70.navy.mil
ctr.navy.mil
ctrnavy.mil
cuervo.jose2.mil
curtis.b.dotson2.mil
curts.navy.mil
cv63.navy.mil
cvn-76.navy.mil
cvn65.navy.mil
cvn68.nacy.mil
cvn68.navy.mil
cvn69.navy.mil
cvn70.navy.mil
cvn71.navy.mil
cvn72.navy.mil
cvn73.navy.mil
cvn74.navy.mil
cvn75.navy.mil
cvn76.navy.mil
cvn77.navy.mil
cvw1.navy.mil
cvw14.navy.mil
cvw2.navy.mil
cvw3.navy.mil
cvw5.navy.mil
cvw9.navy.mil
cybercom.mil
d11.uscg.mil
d7taclet.uscg.mil
dan.harris.mil
dan.mil
daniel.l.mil
daniel.lind.mil
danny.m.adams6.mil
david.a.king.mil
david.c.buchanan.mil
david.g.foss.mil
david.m.esquive16.mil
david.r.doan2.mil
david.villas.mil
davis.navy.mil
dcma.mil
ddg-roosevelt.navy.mil
ddg.navy.mil
ddg100.navy.mil
ddg101.navy.mil
ddg102.navy.mil
ddg103.navy.mil
ddg104.navy.mil
ddg106.navy.mil
ddg107.navy.mil
ddg108.navy.mil
ddg109.navy.mil
ddg110.navy.mil
ddg111.navy.mil
ddg51.navy.mil
ddg52.navy.mil
ddg53.navy.mil
ddg54.navy.mil
ddg55.navy.mil
ddg56.navy.mil
ddg57.navy.mil
ddg58.navy.mil
ddg59.navy.mil
ddg60.navy.mil
ddg61.navy.mil
ddg62.navy.mil
ddg63.navy.mil
ddg64.navy.mil
ddg65.navy.mil
ddg66.navy.mil
ddg67.navy.mil
ddg68.navy.mil
ddg69.navy.mil
ddg70.navy.mil
ddg71.navy.mil
ddg72.navy.mil
ddg73.navy.mil
ddg74.navy.mil
ddg75.navy.mil
ddg76.navy.mil
ddg77.navy.mil
ddg78.navy.mil
ddg79.navy.mil
ddg80.navy.mil
ddg81.navy.mil
ddg83.navy.mil
ddg84.navy.mil
ddg86.navy.mil
ddg87.navy.mil
ddg88.navy.mil
ddg90.navy.mil
ddg91.navy.mil
ddg92.navy.mil
ddg93.navy.mil
ddg94.navy.mil
ddg95.navy.mil
ddg96.navy.mil
ddg97.navy.mil
ddg98.navy.mil
ddg99.navy.mil
decatur.navy.mil
denewc.ang.af.mil
denver.navy.mil
derrick.c.gosney.mil
devin.w.allred4.mil
dfas.mil
dfd.whs.mil
dgg95.navy.mil
dia.mil
disa.mil
dla.mil
dm.af.mil
dma.mil
dobbins.af.mil
donald.r.workman6.mil
dover.af.mil
doyleffg39.navy.mil
dpg.army.mil
dsca.mil
dsd.mil
dtic.mil
dtra.mil
dubuque.navy.mil
dubuque.usmc.mil
dustin.m.parker.mil
dyess.af.mil
eb.mil
eddie.mil
edgar.h.valdez.mil
edwards.af.mil
edwin.s.bender.mil
edwin.t.rosales.mil
eglin.af.mil
eglin.f.mil
eielso.af.mil
eielson.af.mil
eisenhower.navy.mil
eisnehower.navy.mil
elementary.mil
ellsworth.af.mil
elmendorf.af.mil
elrod.navy.mil
embassy.afgn.army.mil
en.mir.a.mil
enterprise.navy.mil
eric.k.johnon1.mil
eric.rodriguez14.mil
eric.s.parks2.mil
eric.s.smith20.mil
escort.mil
essex.navy.mil
ethan.t.dutton.mil
eu.navy.mil
eucom.mil
eur.army.mil
fa.mil
fairchild.af.mil
fe.navy.mil
ffg.57.navy.mil
ffg28.navy.mil
ffg29.navy.mil
ffg32.navy.mil
ffg33.navy.mil
ffg36.navy.mil
ffg38.navy.mil
ffg39.navy.mil
ffg40.navy.mil
ffg41.navy.mil
ffg42.navy.mil
ffg43.navy.mil
ffg45.navy.mil
ffg46.navy.mil
ffg47.navy.mil
ffg48.navy.mil
ffg49.navy.mil
ffg50.navy.mil
ffg51.navy.mil
ffg52.navy.mil
ffg53.navy.mil
ffg54.navy.mil
ffg55.navy.mil
ffg56.navy.mil
ffg57.navy.mil
ffg58.navy.mil
ffg59.navy.mil
ffg60.navy.mil
ffg61.navy.mil
ffg8.navy.mil
filipe.mil
fireblade.mil
fitzgerald.navy.mil
fljack.ang.af.mil
fmmc.army.mil
ford.navy.mil
forscom.army.mil
franciscleversy.af.mil
frank.mil
frankie.heggins.mil
futenma.usmc.mil
g.army.mil
ga.ngb.army.mil
gaba.mil
gabriele.giorgino.mil
gamail.mil
gandi.mil
garobi.ang.af.mil
gary.navy.mil
gasava.ang.af.mil
gates.navy.mil
gene.w.newcomb.mil
germantown.navy.mil
gettysburg.navy.mil
gg.mil
ghosted.mil
gi.af.mil
giannis.mil
gimail.af.mil
gimail.mil
gimil.af.mil
global.mil
gmail.af.mil
gmail.mil
go.army.mil
governor.usn.mil
grandforks.af.mil
gregory.b.baugh.mil
gregory.m.sheehan3.mil
groves.navy.mil
gruboston.uscg.mil
grucharleston.uscg.mil
gruftmacon.uscg.mil
gruohiovalley.uscg.mil
gunston-hall.navy.mil
gunter.af.mil
hajek.mil
halsey.navy.mil
halyburton.navy.mil
hanscom.af.mil
harpers-ferry.navy.mil
harry.c.harper.mil
hawes.navy.mil
health.mil
hell.mil
henry.ruiz.mil
hickam.af.mil
higgins.navy.mil
hil.af.mil
hill.af.mil
hiram.a.barbosa.mil
hmx-1.usmc.mil
hoa.usafricom.mil
holloman.af.mil
hopper.navy.mil
hot.mil
hq.southcom.mil
hqda.army.mil
hqmc.usmc.mil
hs151.navy.mil
hue-city.navy.mil
hurlburt.af.mil
i-mef.usmc.mil
id.ngb.army.mil
ignet.army.mil
iiimef.usmc.mil
iimef.usmc.mil
il.spri.af.mil
imef.usmc.mil
in.ngb.army.mil
infrator.mil

inftwa.ang.af.mil
ingraham.navy.mil
iraq.centcom.mil
ivan.a.urioste.mil
iwo-jima.navy.mil
izmir.af.mil
j.mil
jacob.r.guevara.mil
james.a.emmons.mail.mil
james.m.burks.mil
james.p.sprouts.mil
jash.mil
jason.c.scott.mil
jchung.mil
jcse.mil
jdec-m.isg.mil
jeremy.e.atchison.mil
jeriah.w.horsley.mil
jesse.l.holt4.mil
jesse.m.bevil.mil
jessy.m.petrone.mil
jfcom.mil
jhacker.mil
jiatfw.pacom.mil
jimmy.riley1.mil
jmf.navy.mil
joe.a.castillo18.mil
joel.mil
john.j.shaughnessy4.mil
john.m.baker1.mil
john.s.wood.mil
johnathan.g.george.mil
johnathan.r.mcsperritt
➥.mil
jonathan.d.williams82
➥.mil
jonathan.h.browning.mil
jose.a.rodriguez6.mil
joseph.v.compton.mil
joshua.c.murphy.mil
jsf.mil
juan.m.rivera26.mil
juan.ocasioborrero.mil
justin.d.mcvay.mil
justin.m.salazar.mil
juston.l.silcox.mil
kadena.af.mil
kaio.mil
karioca.mil
kauffman.navy.mil
kcs.mil
kearsarge.navy.mil
keesler.af.mil
kelley.r.callaway.mil
kelvinbennd.mil
kennedy.navy.mil
kenneth.r.witt2.mil
kenny.d.harper2.mil
kevin.n.walker.mil
kevin.w.moss.mil
kira.n.crocker.mil
kirtland.af.mil
kitty-hawk.navy.mil
kjkos.mil
klakring.navy.mil
knox.army.mil
kuwait.swa.army.mil
ky.ngb.army.mil
kyle.m.stephenson.mil
kyle.r.ivory.mil
kyle.w.galloway.mil
kyloui.ang.af.mil
laboon.navy.mil
lackland.af.mil
lake-champlain.navy.mil
lake-erie.navy.mil
lakenheath.af.mil
lamadd.navy.mil
lanewo.ang.af.mil
langley.af.mil
lassen.navy.mil
laughlinaf.mil
lcc19.navy.mil
lcc20.navy.mil
ld49.navy.mil
lee.army.mil
lee.e.george.mil
leytegulf.navy.mil
lha.navy.mil
lha1.navy.mil
lha3.navy.mil
lha4.navy.mil
lha5.navy.mil
lha6.navy.mil
lhd.navy.mil
lhd1.navy.mil
lhd2.navy.mil
lhd3.navy.mil
lhd4.navy.mil
lhd5.navy.mil
lhd6.navy.mil
lhd7.navy.mil
lhd8.navy.mil
lincoln.navy.mil
littlerock.af.mil
llha4.navy.mil
lpd.17.navy.mil
lpd10.navy.mil
lpd13.navy.mil
lpd15.navy.mil
lpd15.nay.mil
lpd17.navy.mil
lpd18.navy.mil
lpd19.navy.mil
lpd21.navy.mil
lpd22.navy.mil
lpd25.navy.mil
lpd7.navy.mil
lpd8.navy.mil
lpd9.navy.mil
lsd38.navy.mil
lsd41.navy.mil
lsd42.navy.mil
lsd43.navy.mil
lsd45.navy.mil
lsd46.navy.mil
lsd47.navy.mil
lsd48.navy.mil
lsd50.navy.mil
lsd51.navy.mil
luis.o.solisrivera.mil
luke.af.mil
luke.mil
macdill.af.mil
magno.eb.mil
mail.mil
mail.ports.navy.mil
mail.umhb.mil
mail.us.army.mil
mail1.monmouth.army.mil
mal.mil
manpower.usmc.mil
marc.anthony.mil
marcello.m.digerlando
➥.mil
marcent.usmc.mil
march.af.mil
marcios.mil
marine.usmc.mil
marines.usmc.mil
mario22.mil
mark.e.ganey.mil
mason.ddg87.mil
mason.navy.mil
massimo.mil
matava.mil
matthew.g.eaton2.mil
matthew.l.weeks2.mil
matthew.phelps4.mil
matthew.r.jacobsen.mil
matthew.s.hicklin.mil
maurice.a.tipton2.mil
maxwell.af.mil
mcaap.army.mil
mcalaja.mil
mcbbutler.usmc.mil
mcbh.usmc.mil
mccain.navy.mil
mcchord.af.mil
mccraw.mil
mcguire.af.mil
mcinerney.navy.mil
mcm1.navy.mil
mcm10.navy.mil
mcm11.navy.mil
mcm14.navy.mil
mcm3.navy.mil
mcm4.nav.mil
mcm4.navy.mil
mcm6.navy.mil
mcm7.navy.mil
mcm9.navy.mil
mcrc.usmc.mil
mcsftco.nsanwannex
➥.navy.mil
md.ngb.army.mil
mda.mil
me.navy.mil
med.navy.mil
menwithhill.af.mil
mepcom.army.mil
mercy.navy.mil
mesa-verde.usmc.mil
mfp.mil
mfr.usmc.mil
mgmc.af.mil
mi.army.mil
michael.a.giglio.mil
michael.d.moyer1.mil
michael.j.ong2.mil
michael.l.evans48.mil
michael.p.dwyer3.mil
michael.r.lewis1.mil
michael.r.richardson10
➥.mil
migue.mil
miguel.a.barud.mil
mil.dos.mil
mil.mail.mil
mildenhall.af.mil
milius.navy.mil
miramar.usmc.mil
misawa.af.mil
misouri.navy.mil
mitscher.navy.mil
mmcs.army.mil
mmso.med.navy.mil
mndulu.ang.af.mil
mnstci.iraq.centcom.mil
mnstpa.ang.af.mil
mobile-bay.navy.mil
monteiro.mar.mil
monterey.navy.mil
moody.af.mil
morgenthau.uscg.mil
mountainhom.af.mil
mountainhome.af.mil
ms.ngb.army.mil
msc.navy.mil
msjack.ang.af.mil
mstp.quantico.usmc.mil
mustin.navy.mil
na.amedd.army.mil
naskef.navy.mil
nassau.navy.mil
nassay.navy.mil
nathan.r.boehm.mil
nathanial.f.myers.mil
navair.navy.mil
navsoc.navy.mil
navsoc.socom.mil
navt.mil
navy.med.mil
navy.mil
nayv.mil
ncf.navy.mil
ncis.navy.mil
ndo.navy.mil
nellis.af.mil
nemof.naples.navy.mil
nesucharleston.uscg.mil
ng.army.mil
nga.mil
ngb.army.mil
nhcne.med.navy.mil
nhcorpus.med.navy.mil
nhgl.med.navy.mil
niagarafalls.af.mil
nicholas.fontaine.mil
nimitz.navy.mil
nj.ngb.army.mil
njatla.ang.af.mil
nmci.usmc.mil
nmcsd.med.navy.mil
nmic.navy.mil
nnsy.navy.mil
npt.nuwx.navy.mil
nrl.navy.mil
nrlssc.navy.mil
nro.mil
nsa.naples.navy.mil
nsn.cmar.navy.mil
nswc.navy.mil
nswccd.navy.mil
nsweast.socom.mil
nswlant.navy.mil
nt.quantico.usmc.mil
nv.ngb.army.mil
nvl.army.mil
nvreno.ang.af.mil
nw.amedd.army.mil
nwc.navy.mil
ny.ngb.army.mil
nyniag.ang.af.mil
nyscot.ang.af.mil
nystew.ang.af.mil
offutt.af.mil
ogden.navy.mil
ogn.af.mil
oh.ngb.army.mil
ohmans.ang.af.mil
ohspri.ang.af.mil
oktuls.ang.af.mil
osan.af.mil
osprey.navy.mil
osvaldo.garcia1.mil
otc.army.mil
pa.ngb.army.mil
pacom.mil
pasadena.navy.mil
patrick.af.mil
paul.a.mason6.mil
paul.t.girdley.mil
pba.army.mil
pcola.med.navy.mil
pcola.navy.med.mil
pearlharbor.usmc.mil
peleliu.navy.mil
pendeleton.usmc.mil
pendleton.usmc.mil
pentagon.af.mil
peque2.mil
peterson.af.mil
pfpa.mil
philippine-sea.navy.mil
pica.army.mil
pil.mil
pinckney.navy.mil
pittsburgh.af.mil
ponce.navy.mil
ponce.usmc.mil
pope.af.mil
port-royal.navy.mil
porter.navy.mil
preble.navy.mil
pretinha.mil
psns.navy.mil
pug.mil
radium.ncsc.mil
ramage.navy.mil
ramstein.af.mil
randolph.a.matz.mil
randolph.af.mil
ray.a.preston2.mil
raymond.h.paquin.mil
re.mil
reginaldo.mil
rellie.z.lorenzo.mil
rex.rosales.mil
rgb49.navy.mil
rich.mil
richard.d.hecht.mil
richard.oquendo.mil
riquon.ang.af.mil
robert.d.sanson.mil
robert.l.stone87.mil
robert.p.canfield.mil
roberto.j.lopez22.mil
roberto.mil
roberts.navy.mil
robins.af.mil
rocketmail.mil
ronisantos.mil
roosevelt-ddg.navy.mil
roosevelt.navy.mil
rosado.mil
ross.navy.mil
rrmc.army.mil
rs.af.mil
rubayat.mil
rubenziitooh-trilloz.mil
rucker.army.mil
rushmore.navy.mil
ryan.d.wilson14.mil
ryan.h.lavrusky.mil
s.army.mil
saipan.navy.mil
salvi.mil
san.osd.mil
sandro.mil
sandyhook.uscg.mil
sanjacinto.navy.mil
sasebo.navy.mil
schriever.af.mil
scott.a.miller.mil
scott.af.mil
scott.d.vetterman.mil
scott.disa.mil
scott.m.roberts.mil
scout.navy.mil
scranton.navy.mil
scrmc.navy.mil
sddc.army.mil
se.amedd.army.mil
seabee.navy.mil
sean.m.odea10.mil
sean.p.carleo.mil
seba.mil
sedux.mil
sellis.mil
sembach.af.mil
sentry.navy.mil
seymourjohnson.af.mil
seymourjonson.af.mil
sfsgt.marden.us.army.mil
shaw.af.mil
sheppard.af.mil
shiloh.navy.mil
shoup.navy.mil
shreveport.navy.mil
simpson.navy.mil
sldkflww.mil
slidell.disa.mil
soar.army.mil
soc.mil
socom.mil
sony.siete.mil
space.nrl.navy.mil
spangdahlem.af.mil
spawar.navy.mil
spcaf.af.mil
ssn21.navy.mil
ssp.navy.mil
stanewhaven.uscg.mil
stapascagoula.uscg.mil
stennis.navy.mil
steve.d.elliott.mil
steven.h.dotterer.mil
steven.m.francis14.mil
stout.navy.mil
stratcom.mil
stripes.osd.mil
su.army.mil
sullivans.navy.mil
supshipnn.navy.mil
swa.af.mil
swa.army.mil
swflant.navy.mil
swfpac.navy.mil
t.mil
tacom.army.mil
tarawa.navy.mil
tarawa.usmc.mil
tavo.mil
taylor.navy.mil
techrep.navy.mil
tecom.usmc.mil
thach.navy.mil
thaddeus.c.chabior2.mil
the.mil
thomas.e.blair.mil
thomas.p.peters.mil
tiffanyjohnson127.mil
timothy.b.castine.mil
timothy.s.withers.mil
tinker.af.mil
tinker.at.mil
tnmemp.ang.af.mil
toledo.navy.mil
tomasek.mil
tony.mil
tortuga.navy.mil
training.navy.mil
tramal.c.williams2.mil
travis.af.mil
travis.b.malena.mil
travis.sweatt.mil
travis.w.bohannon.mil
trenton.navy.mil
trevor.r.ladd.mil
trey.l.weaver.mil
truman.mil
truman.navy.mil
tx.ngb.army.mil
txelli.ang.af.mil
tyler.j.whiteman.mil
tyndal.mil
tyndall.af.mil
u.s.army.mil
u.s.mil
ua.army.mil
ud.army.mil
umcs.mil
un.army.mil
underwood.navy.mil
us.af.mil
us.airforce.mil
us.amry.mil
us.amy.mil
us.arm.mil
us.armt.mil
us.armty.mil
us.army..mil
us.army.amedds.mil
us.army.mil
us.army.smil.mil
us.armyl.mil
us.arny.mil
us.arrmy.mil
us.ary.mil
us.gov.mil
us.mail.mil
us.med.navy.mil
us.mil
us.rmy.mil
us.srmy.mil
usac.army.mil
usace.army.mil
usace.mil
usaemy.mil
usafa.af.mil
usafricom.mil
usamry.mil
usar.army.mil
usarec.army.mil
usarmy.com.mil
usarmy.mil
usc.mil
uscg.mil
uscg.munro.mil
usmarmy.mil
usmc.mil
usmtm.sppn.af.mil
usn.mil
ussharrystruman.navy.mil
ussmc.mil
usspearlharbor.navy.mil
usspearlharbor.usmc.mil
ustranscom.mil
usuhs.mil
utsalt.ang.af.mil
vance.af.mil
vanesa.mil
varich.ang.af.mil
vaw126.navy.mil
vb.socom.mil
vella-gulf.navy.mil
venus.mil
vfa82.navy.mil
vfa86.navy.mil
vickburg.navy.mil
vicksburg.navy.mil
victor.e.chavez.mil
vinson.navy.mil
vlad.mil
vs.army.mil
vtburl.ang.af.mil
wa.ngb.army.mil
warren.af.mil
warrior.navy.mil
washington.mil
washington.navy.mil
wasp.navy.mil
wataco.ang.af.mil
westover.af.mil
whalenskyler.1rbn.mil
whidbey-island.navy.mil
whiteman.af.mil
whs.mil
wicrtc.ang.af.mil
william.a.feldhahn2.mil
william.e.winstead.mil
william.j.daugherty.mil
william.p.corley.mil
willian.mil
willie.h.wallace.mil
willy.mil
wimilw.ang.af.mil
wpafb.af.mil
wva.army.mil
wvchar.ang.af.mil
xa.mil
yahoo.mil
yokota.af.mil
yorktown.navy.mil
youngstown.af.mil
ytroi.mil
yuma.army.mil
zachary.k.hinton.mil

by mmx3

This article is for information purposes only and is not intended to be misused in any way to compromise the security of the facility.

This article was inspired by the 29:3 article on the BOP technology. Should you ever find yourself in here, you'll have knowledge of what is available to play with, though obviously I advise against doing so as a disclaimer. I have had no luck in the discoveries written here in terms of something useful like getting free calls or accessing the Internet, but hopefully in sharing this, if any reader *does* end up in this place (more likely than you think if you're caught federally and then "cooperate" - I am uncooperative), you'll have a starting point to try and further my discoveries.

Queens Private Detention Center is owned by The GEO Group Inc. (Google things that look interesting here for more information), a company that is building more and more jails in more and more countries. It mainly houses rats, some of whom are "criminals with hacker capabilities," not hackers, a distinction most people seem to not be able to make. The rest are gang bangers telling on their friends and immigrants awaiting deportation. So if you end up "cooperating" with the feds, you'll likely come here to this old postal storage warehouse converted to a makeshift jail with seven dorms and a small total of 245 detainees. They do not read incoming or outgoing mail here, just a quick little look at what comes in when they open it in front of you. Let's begin with the phones.

Phones - Mukinabaht

The phones are not labeled with any kind of model number or such, but have the traditional handheld unit that you find on payphones everywhere. That connects to a silver housing about 8x20 and extending four or so inches out from the wall. There's a blue button for volume levels at the top left, next to a sign that says 1 - English, 2 - Spanish, and 3 - Vietnamese (!?}, an option not actually available; and "All calls are subject to monitoring and recording - Global Tel Link."

Picking up the handset, you hear: [Start here when you read "Resets call"] "For English, press 1 [place Spanish here], numero dos." So that's 1 and 2. Let's press 9! "One hundred seven, one hundred seven" - depending on what phone you're on, the number will be different; three phones in a row, three sequential numbers. [Resets call, pressed 1 for English] "For a collect call, press 0. For a debit call, press 1 (and in a different woman's voice). For debit card information, press 8." That's 1,0, and 8. [Pressed 3] "Enter the card you want to transfer funds from now." This option allows you to enter an eight-digit detainee ID number (i.e., 12345-053, where 053 is Eastern District and 054 is Southern, etc. Entering any detainee number you happen to know will allow you to know how much money they have in their account. After that information is spoken, the phone states "Enter the card you want to transfer funds to now." [enters next ID] It tells the amount remaining, then (in a third and sinister woman's voice) "Transfer funds... is not allowed. Goodbye." (The kind of goodbye you'd hear before receiving a fatal bullet to the head.) This promptly freezes the second phone account (apologies to test subject) until the next day. In short, this function is disabled and is only "useful" for spying on someone else's remaining funds. The second ID number I used for testing is 12346578, which, I'm assuming is a test account which always has one dollar, and no registered numbers that I know of.

[Resets call, 1 - English, pressed 2 - nothing, pressed 4] The phone pretends to transfer a call somewhere, and then says "No calls are allowed at this time." [Pressed 5 - same as 0, pressed 6] "That is not an authorized number. Please try again later." (Yeah. Because with time, it might suddenly become authorized. No.)

Brief digression: Way back in the beginning of MP3 file sharing on Audio Galaxy (remember it?), you could put MP3s in your shared folder

of songs that weren't available on search (such as personally recorded projects) and make them appear on search simply by searching it after putting it in the folder, instead of going through the upload process which could take not only a long time but not even work as well. So they would "suddenly become authorized" by using my method. Right. Anyway.

[Pressed 7] "Thank you for using Global Tel Link's inmate phone services." [pressed 8] "Local debit calls will cost $1.35 for the first minute, 6 cents each additional minute. Intra-LATA calls are 28 cents a minute, 49 cents each additional minute...." [Pressed 9, then *, then #] "No calls are allowed at this time." All responses are the same in the Spanish menu.

[Resets call, 1 - English, pressed 0 - collect call] "Enter your ID and 4 digit PIN number now." [complies] "Enter..." phone number [pressed #777] [new woman's voice] "Thank you for calling the U.S. Department of Homeland Security of the Inspector General's Hotline. Press 1 for English." [Pressed 1] This allows you to report allegations of employee corruption, misuse of [place list here], abuse, etc. [Pressed 0, not an option given] This will transfer you to an operator who, circa 2010, would not know where we were calling from and thus we could get her to give us an outside line. Free calls! I would imagine this does not work anymore because, like with all good exploits, everyone abused it and things change as a result.

In order to add a number to your phone list you must, stupidly, write it on an "add phone number" request sheet which is then left in the podium that the CO occasionally sits at until the "phone guy" (I teach him how to fix problems, the idiot) picks it up and adds it into the server upstairs. So, if I know your four-digit PIN, I could (and this happened recently and got someone box time (box - a lonely cell in segregation)) add one of my numbers to your list, use the 3 option from above, check how much money you have on your account, then make some phone calls to some far away location.

Another exploit was having someone buy a Black Card (a calling card available at bodegas) with a local area code (i.e., 718) on it, and then the detainee would add that number to his list, call it, and be billed locally for calls anywhere because calling the card would bring you to a menu of its own options where you would enter a number to call. This too got around, was abused, and "phone guy" changed the settings in the server to disconnect calls where buttons were pressed during conversation (conversation is initiated upon connection of the original dialed number). No more calling cards.

Three-way calling occasionally works, but is not allowed. Sometimes the call will be recorded blatantly when the woman's voice announces such. I'm guessing trigger words are the cause but I have not experimented. When you call someone, what appears on their caller ID is always different but, as a real example: "713.489.7846 Unavailable" - which is a Texas area code. When you hang up or disconnect, the phone woman says "Thank you for using PCS." (PCS?) Transferring funds to the phone is done with the commissary computer in each unit which we'll discuss shortly.

There is a small blue phone in each unit about 8x16 and extending out about four inches from the wall which the COs use to call each other and Control (more on Control later). They use two-digit numbers (i.e., 15). There are other line phones in other areas of the building (as an "employee" I see it all) which require you to dial 9 before the number you want to dial.

If you go to "phone guy" (write a request), you can get a printout of your authorized phone numbers. On that sheet in the top left corner it says "PCS/GTL." The first column is "PAN" and shows all the numbers. The next column is "Blocked - Yes/No." Next is "Active - Yes/Disabled," then "Relationship," which says "Other" for all numbers. Beautifully, at the bottom of the page is: `http://10.200.103.25/pinpan/➥print_pin_basic_detail.asp?cmd➥=edit&pin=xxxxx053&PrintA`. You know that the five x's are part of the detainee number and, as we're all savvy here, I don't need to bore you with explanations about the 10 or the -asp. You can also have printed up recent call history which shows exactly what phone and dorm you're on/in, who terminated the call, call length, number, date and time, and of course the server's IP address, etc.

Computers - Telephasic Workshop

Starting with the commissary computers, of which there is one in each of the seven units here, I'll describe all that I'm able to about all the computers I've seen/played with. So on the wall housed in a black/gray box with two black circular locks (similar to an elevator keyhole) is a 13 inch touchscreen which, when not in use, has an interesting screen saver. At one second

intervals for a total of six, different colored portions of a circle are filled in until the fifth second when it displays Cobra Kiosk. If you touch the top left corner, you can freeze in place a nice color pattern, as I strangely like to do particularly when there are blue and green colors - which we do not see otherwise. Holding the top left corner does not result in a menu. The satellite (I refer to any PC in a network connected to a server as a satellite - I just like to!) is powered by a three-pronged white cable which, if you unplug then plug in resets the machine which then reveals a black screen with Dell, then a Windows XP screen, then a blue screen with HP top right, then a Windows XP Embedded screen, then a white screen with a Start button on the task bar below which cannot be engaged with touching.

So this is the Cobra Kiosk. Underneath in part of the housing in a recess is a fingerprint scanner which says TouchChip on it. So the order of operations to gain access is: touch the screen (displays two tabs - "Cobra Resident Services" and "exit"). [Pressed "CRS"] This goes to a language selection screen with date and time at top left: English, Creole, French, Hmong, Spanish - a strange assortment. There should be Russian and Chinese since there are so many of them here. [Pressed English] You are presented with two tabs: "Facility Information" (unavailable) and "Cobra Kiosk Login." [Pressed Login] You are shown a keypad with 0-9 arranged like a phone pad with tabs under it for cancel, continue, and backspace. Here you will enter your eight-digit ID number, hit "continue," then place your finger (one that you've assigned to the machine's memory) for verification, then do your business. But ah, not so fast. We were given the opportunity to enter numbers on a screen! Albeit entirely useless to do so, here is what I've found.

The keypad allows you to enter up to 15 numbers. That's 15 zeroes through 15 nines - one quadrillion possible entries! Ouch! Well, I found a few after months of endless boredom. If you enter eight zeroes, or seven zeroes and a one, then hit continue, it says "Account has been suspended!" These used to take you to an "enter date of birth" screen - which seven zeroes and a two now does. The format is xx/xx/xxxx and is satisfied by means of entering numbers with the pad, obviously. I've found no birthday which allowed me access, but the computer will allow infinite guesses. Seven zeroes and a three takes you to the fingerprint scan screen. Presumably, none are registered as I receive a "No match" screen. Entering 15 ones used to go to the fingerprint screen, but that is now suspended as well. I've found nothing else worth mentioning. I told "phone guy" about all these, thinking he would be in the know, so of course he wasn't and thought I was smart for finding it - duh-weeb.

I'm guessing that the satellites are connected to the same server as the phones as this is how you transfer funds to your phone account. The option to "order commissary" is offline from midnight Tuesday until noon that day. Commissary comes from Swanson Services Corp., the Delaware Service Center, and this time offline is when the orders "go out" - which tells me that some work is done manually to facilitate the transfer of accumulated orders through the Internet. One time they were updating pricing and on the screen in the unit we could see exactly what the programmer (assumed) saw on the server's desktop. He flew through the folders until he got to some script which appeared to be SQL (too quick to get a good look), scrolled down, and edited it at light speed, then issued a reset. I did not have pen or paper at the time, so I have no notes for this.

Logging in normally (finally), allows you to do one other very useless thing. On any screen if you touch the top left and slide your finger slightly, everything becomes highlighted in blue as if Select All-ed. You can then drag everything up about half an inch, allowing you to do absolutely nothing else! I know, such excitement. We don't need to detail what you can buy as that's very boring, but you can view receipts for past purchases and deposits, buy food, notepads, sundry, blah, blah, blah. Next!

There are five computers in the law library. Three are wall mounted touchscreens (satellites!) connected to a Dell PowerEdge T110 standalone server in the next room which we don't go in. On those screens appears TST Touch Sonic Technologies, subsidiary of Touch Legal, Inc. running on Windows 7 Professional. The touchable tabs on the screen are Lexis/Nexis Law Library, Lexis/Nexis Video Tutorial, reference tools, and an inmate reference document tab. If we touch on the video tutorial, it brings up a Windows Media Player on the right with one choice of video on the left. If we hold a finger to the screen on the player, a menu appears, at the bottom of which are Options, Details, Help, etc. When Help is tapped, it brings you to the WMP help dialog

screen, where you then click on an online link, then interrupt it to go to the desktop. All sorts of fun to be had when you can access everything in the computer unhinged Unfortunately, none of it equals Internet capabilities. It is physically not connected to the Internet.

There is a desktop for printing legal and personal letters. Some people try to hide their files by changing the viewable files in folder options. Bums! There is another desktop for viewing discoveries (evidence pertaining to your case). The two desktops end up getting messed up from idiots who don't know how to do anything with a computer, but proceed to play with it anyway, and get switched out often, so to describe anything about them is senseless. Right now, there is a Dell and a Compaq that look like they came straight from the shelf at the local Best Buy, running Windows 7 and XP. There's nothing fantastic, no connections or special programs. The discovery computer though, thanks to the best exploit pulled yet - which I've shared with no one but you dear reader - has been instrumental to my sanity. Details in a moment ("patience, Iago"}. Around the facility are *a* few more Dell Dimensions with Internet access (medical, intake, etc.), none of which I've been able to play on.

There are two printers in the law library - a Brother HL-2270 DW Series with 802.11b/g Wi-Fi and an HP LaserJet P2035. Boring. You probably know all about the Brother printers and the minimal fun you can have with it.

Cable Boxes - Chromakey Dreamcoat

Each unit has two cable boxes, Samsung SMT-H3050s. They suck. When you use the B button on the remote to try and search for shows, pressing the D-cursor too quickly sends the box into panic mode, where it brings up a diagnostics screen. Here you can scroll through 22 screens of information, including the box's IP address and uber-tons of other I-don't-know-data. Other dorms have different boxes, some with USB 2.0 slots. Some people have had flash drives with cheap Dominican porn on them that used to circulate. That covers the cable.

Control - Into the Rainbow Vein

Control is a well-guarded room in the center of the building. In it is a row of monitors for the 60 plus cameras around the building and three touchscreens with Windows interfaces. These control the doors and cameras in the entire facility, except for one door - the front one - which is manually opened with a large, flat key. On a CO's radio (walkie-talkie) he/she will announce "Control, door 30" and an officer in Control will touch door 30 on the screen and it will open. The lock mechanism slides downward on an angle, retracting into the door frame. It will pause and then extend back into locking position. If you miss it, you radio again or press a button next to the door on a silver intercom box and Control will hit the door.

The computers in Control and the Dell in the Tour Commander's office (where the T110 is next to the library) are connected to each other, allowing them to review footage of fights or whatever else they need to look at. As far as I know, the system to control the doors is closed to outside connections. However, as mentioned (I did mention it, I think?) the TC's PC is Internet accessible and *it* is connected to Control. The only link unknown is whether it connects to the touchscreens controlling the doors. If so, and this wouldn't surprise me, then the system can be compromised and controlled externally. Now wouldn't that be ridiculous if suddenly all the doors just started constantly unlocking? The chief of security here watches the cameras from home via the Internet. It's not unrealistic to think that someone outside could take control of the doors and cameras and arrange one's escape. However, there two armed marshals in a white van 24 hours a day that patrol the perimeter. *Do not* screw around with this information, lest ye cross the line from hacker to criminal, feel me?

Best Exploit - Open The Internal Eye

"Dear discovery computer, me and you have shared some very intimate and secret times together. Thank you." No one knows what I am about to write about. The discovery computer is where one goes to review text, audio, and video of evidence in their cases, usually recordings made by informants who were wired. They come on DVDs or CDs which go to classifications where they sit until they call the detainee to come to the library to review it. You bring your headphones and plug into the 1/8 inch jack and get busy. Of course, you know where I'm going with this, right? What? Review other people's discoveries that were automatically or idiotically added to the computer's memory? Hell no! Who the hell cares about that?

In this wasteland, all we have is a radio; no MP3 players or CD players. So I simply had a friend outside make an MP3 disc of my

favorite new and old music (Boards of Canada - *Geogaddi,* Wormed- *Exodromos,* Autechre - *Xi,* Cryptopsy, Arovane, Iron and Wine, just to name a few for you to check out), had him label the disc with my full name, my ID number, and "discovery" on it, put it in an envelope that was labeled with my attorney's return address, the address of the facility with my full information, and the words "legal mail" all over it. When this "legal mail" comes in, only I can view the contents of the disc. So here I am writing this article for ya'll, in jail, listening to the new Ulcerate album (which is maniacally technical, abrasive, and brutal). Anyone who comes in here while I'm doing this thinks I'm taking notes on my case!

One Very Important Thought

I cannot end this piece without mentioning a more consistent variable that helps me get through this time. The radio, diminutive though it may seem, provides me with *Off The Hook,* which is brought to us all by WBAI and WBAI.org. Everyone outside the New York tri-state area can listen online, and so technically can those of us within range, *but,* radio is an extremely important medium in reaching people more broadly. It is more easily accessible while walking, working, or driving and carries more of a punch when political, conspiratorial, medical, etc., views that are not shared on mainstream radio can still come across New York City because of WBAI. The things that we all read and write about in these very pages and more are always discussed on air here. Therefore, as a community, it becomes our responsibility to help support platforms that provide stages for the sharing of important topics and issues.

WBAI is listener supported radio and depends on the contributions of its listeners for it to continue to provide coverage of topics that will never be discussed elsewhere. Right now the radio station is in some very tough financial times and I'm sure that Big Brother is trying its hardest to get it off the air as well somehow. Knowledge is power, the kind of power that the feds do not like. This station is a hacker's platform on many levels. I ask the readers of this article, which of course was inspired by *2600* but even more so by WBAI and *Off The Hook* and the weekly reminder it is to me to be a functioning part of its existence, to consider making a contribution - even if you haven't listened to the station - at `wbai.org`. Support the scene however you can! Thanks for reading!

Open Source Repository Abuse

by Terrible Doe

Open Source Software (OSS) has been firmly established as a viable software development and licensing model. Developers love the collaboration and the ability to reuse existing code while users appreciate free software that can compete with commercial applications. Most people tend to see OSS as a complete win-win situation. Unfortunately, from a security perspective this isn't always the case. There have been several recent examples where open source software (or more specifically, open source software repositories) have been at the center of major security breaches. Uber got into bother when a developer accidentally stored a sensitive database key on a publicly accessible GitHub page. The iOS "goto fail" bug was discovered by a security researcher after Apple made the code publicly available.

Developers, whether intentionally or not, sometimes store things they shouldn't on public source code repositories. Some developers believe that it's secure by default or that no one would be looking at their code. Of course, the more people working in that repository, the harder it is to maintain control and the higher the likelihood that some sensitive information could be stored. Even if specific, sensitive data isn't available from the repository, understanding the source code of any application can help in understanding how to attack it.

In this article, I will show what things can be found by digging around in source code repositories. I'll show where to look and how to do the searches. Finally, I'll cover how this information can be used by the intrepid hacker and how to secure it as a developer.

The most obvious source code repository, GitHub, can be a good starting point. Many of the search strings provided later will return results from GitHub. They are looking at improving the security of the site by implementing scrubbers to remove sensitive files. If you find something on GitHub, copy it out or it may be removed the next time you look for it. Other, dedicated repo hosting sites exist as

well. SourceForge, BitBucket, and more can be found by performing a quick search.

Increasingly, tech companies are creating their own source code repositories. Microsoft's Codeplex is a great resource for Windows OSS code. Google has their own Google Code OSS project hosting service as well, but they plan to discontinue that in January 2016 (get at it while you can!).

Apart from these dedicated repositories, many open source projects will host their own public repository. Google's Chromium codebase (which Chrome and Chrome OS are derived from) has a publicly accessible repository, as do many other sponsored projects. Smaller companies and individuals will often do the same. Many individual software developers will make their repositories public as well (at times accidentally).

Using Google to find the hidden repositories is as simple as understanding how the repos are built. Git, a popular repo, will usually end in " .git". A Google of "filetype:git" will give you about 1.4 million repositories (as of this writing). Subversion, another popular repo, uses ".svn" files to store metadata about the source code. Another Google search will help find those as well.

OK, so now you know where to look. What kinds of things can you expect to find in these repositories? Pretty much anything! You can find the private encryption keys for a user/application. There may be information in the code comments, such as test user accounts (they tend to live forever) or the developer's notes on which lines of code are buggy (useful for writing exploits). Configuration files often contain user credentials for the application to use for access (known as functional accounts) or may have URLs to other systems. Since the repositories can version the code, digging into the history of it could reveal things that the developers had included, but then deleted, such as test data or proof-of-concept code. There can be hard-coded information in the code files themselves (known as a magic number).

If the purpose of accessing the source code is to get a better understanding of how the application works, simply browsing through the accessible repository can be enough. To get even more in-depth, you could load the codebase into your development environment and build it yourself. This can tell you where the weak parts of the system may be and how it could be exploited. By compiling it yourself, you can debug the code and step through it to see how various operations are performed. However, if you're not a programmer, then you're probably just interested in what secrets you can find in the code.

Using standard Google advanced search operators (inurl, site, filetype, user) in various configurations will generally provide as much info as needed. Here are some example search queries that will yield interesting results (the search string is after the "="). Also, try changing the target site to other repo sites. This is not a comprehensive list, but should give a good idea of what could be found.

- SSH hosts and keys = `site:github.com ➥ inurl:"known_hosts" "ssh-rsa"`
- Private encryption keys = `site:github ➥.com inurl:"id_rsa" -inurl: ➥"pub"`
- Test configuration info = `site:github ➥.com inurl:"test" filetype:config`
- Ruby on Rails secure token = `site:github.com inurl:secret_ ➥token.rb`
- Windows Azure account keys = `site:github.com ";AccountKey=" ➥ filetype:config`
- Database connection config = `site: ➥github.com ";User Id=" ➥ filetype:config`
- Amazon Web Service access key (Java) = `site:github.com "AWS_ACCESS_KEY_ ➥ID" filetype:properties`
- Amazon Web Service access key (Other) = `site:github.com "AWS_ACCESS_KEY_ ➥ID" filetype:config`
- Bash command history = `site:github ➥.com filetype:bash_history`
- Account config data = `site:github.com ➥ filetype:xml inurl:accounts.xml`
- SQL containing passwords = `site: ➥github.com filetype:sql where ➥ password`
- Django settings file = `site:github.com ➥ inurl:settings.py`

By now, most of you are thinking about other things that you may be able to uncover. As with all things, due care and discretion should be followed before diving in. For example, Uber issued a subpoena to GitHub to force them to provide all of the IP addresses that accessed their secret key. Be smart, be safe, and be informed.

My Voice Is My Key

by GerbilByte

So there I was. I was drafted in to work a second time for a small company (who again shall remain nameless, but for this article we will call the company Bumble Bee Internet Security Services) for several months. Again. As if I'd just copied-and-pasted this opening paragraph from my previous article ("Taking Your Work Home After Work," *2600* 2014-2015 Winter edition - buy the back issue if you've not got it).

This time though it was a much better company - I was basically drafted to penetrate the physical security of a company that required their own securities tested in that area. Basically breaking in to "capture a flag," so to put it. I was asked to see how possible it was to sneak into "Room 123" - there would be an envelope in there taped underneath one of the desks. I took the challenge, not because of the interest I had in security, but it was what I was getting paid to do! The only information that I had was that there were security guards in the building 24/7.

And so my challenge started.

Part One - Information Gathering

At about 08:30 one morning I drove to the target building, parked in a carpark across the road, and watched the activity of its employees for a couple of hours. It was like a police stakeout, but without the coffee and donuts.

The building really was secure. It was surrounded by a large perimeter fence, there was a carpark around the back with paths that led to the main entrance and a small overused smoking shelter. The main entrance was accessible by the public.

I observed the entrance for a few minutes. The main people that were entering the building mostly wore suits and some were in smart-casual. If I was to enter this building, then I'd best be dressed the same way. Some people were carrying holdalls and a couple I noticed were carrying and wearing bicycle helmets. This told me there must be a bike shelter somewhere too!

The smoking shelter contained people smoking, which was bloody obvious. Some were on their own, some were holding drinks, some were young, others old, and some were talking to each other and having a general morning chat. Around the corner from the smoking shelter was a rubbish bin that contained an overflowing ashtray and a recycling bin that overflowed with stacks of empty paper cups. This is where I realize that this article is now sounding like a text adventure game I used to play on my Spectrum. Exits were north, south, and west.

About 09:15, the smoking shelter became more or less empty.

I decided to see what I could from the main entrance without entering the building. It looked very posh! Marble floor, green plants here and there, and at the far end of the corridor was a reception and a security window on the right hand side. Beyond these were card activated barriers that I guessed led to the lifts, stairs, and offices.

Part Two - Putting My Plan Into Action: Phase One

I decided for this job that I would attempt access to the building in the afternoon, but first I would have to get more solid information of the people who worked there, such as names, phone numbers, departments they worked for, etc. How did I go about this?

Well, I came prepared. I wasn't wearing a suit, but I was wearing a shirt, trousers, and smart shoes. In the boot (trunk) of my car I had a tie, my laptop, a briefcase, and a mechanics toolbox containing all sorts of car fixing tools, bulbs, fuses etc. - basically stuff that I wouldn't have a clue how to use if my car should get a puncture, but I digress. The toolbox is irrelevant to this article. What I didn't have was ID for the building, but I didn't expect this to be too much of a problem for me. I put on my tie and went to the nearest shop to buy some cigarettes.

Now, I am not a smoker. I'm more like one of them whingy ex-smokers; I gave up the habit years ago. I also bought an ID badge

holder, but fixed it to my belt in a way that it was permanently "reversed" so that nobody could see the "badge side" of it and returned back to the building with opened cigarette box in hand to chat to a few smokers. I walked towards the smoking shelter, taking a half-full cup from the stack in the recycling bin.

The smoking shelter was empty apart from one bored looking young lady standing on her own, so I went in the corner with my cigarette in my mouth and then awkwardly "searched" with one hand for my lighter, but being a non-smoker I didn't have one.

"Excuse me miss," I said as I approached the girl. "I don't suppose you can let me use your lighter?"

"Of course you can," she replied as she fumbled in her bag. I could see by her pass on her lanyard that her name was Lizzie ****. She passed me her lighter.

"Hey thanks," I smiled as I lit my cigarette and passed her the lighter back. "You look like you're having the time of your life," I joked which was returned by a puzzled look. "My name is Norman. I'm new here," I said quickly and held out my hand.

"Lizzie," she replied and smiled as we shook hands. "We've had quite a few people starting recently."

Well, that was a stroke of luck! A bit more small talk ensued and I found out that she was working on the design team, her boss was called Derek Land and he was away for the week, leaving the team in a bit of a quandary, and also there was another building to the company across town (Herald House). She was situated on the second floor and sat next to a complete knob who called himself Jeremy. I was quite impressed with what information I could extract from just one smoker. After she left, I waited a short while before stubbing out my cigarette, disposing of the cup of whatever-it-was, and returning to my car. The first phase of my plan was complete.

Part Three - Putting My Plan Into Action: Phase Two

Back at home, I had a brew and thought about the next part of my plan, about how I could use the information I had taken and use this for my purpose of getting into the building. In my head, I formed a scenario which turned into a plan. It was risky, but nevertheless I decided to go ahead and try it - after all, I had nothing to lose. Well, nothing but a pay check and a little bit of credibility. I spent the next few hours thinking of the scenario and as many "recovery" plans as I could should any obstacles get presented. What I needed to do though was to print the company's logo onto a small sheet of adhesive paper and stick it on the lid of my laptop so it looked like I belonged there.

In the afternoon, I was ready. Time to return to the building fully suited with a laptop and paper wallet under my arm that contained a few blank pieces of paper. I parked a few streets away and ran to the building to get a bit of a pant (I'm not the world's fittest man, I rate myself about seventh or so) and ran straight up to reception. The lady (Tina) looked up and smiled. "Can I help you?"

"Hi. I'm really sorry but I've just rushed in for an emergency meeting but I've forgotten my pass," I replied.

"Oh, you'll have to go to security and get a temporary one for the day," she said as she pointed across to the security window where I could see several guards watching monitors.

I walked over and was immediately greeted. "What can I do for you, sir?"

"Hi. I was just saying to Tina that I've just rushed in for an emergency meeting when I'm meant to be on leave," I explained with a hint that I knew Tina the receptionist. I only got her name from her badge. "Please can you issue me a temporary pass for the day?"

The security guard smiled and looked away and presented me with a clipboard to enter my details. "Please can I take you name sir?"

Now this was a question. I had a false name made up with a made up job description who wouldn't be on the payroll. I also knew the name of somebody who did exist who wasn't in the office today. I decided to gamble - if I was successful, then the rest of my plan would be plain sailing.

"Derek Land. Manager of the design team."

The security guard looked at me and walked away from the window without saying a word. These are tense moments, especially for a beginner. What seemed about an hour later, the guard returned with a pass in his hand.

"Here you go Derek. Your credentials have been added to this pass, they should be ready in a few minutes. But I can't give this to you," he said as he snapped it back from me. I was done. Task failed. Game Over. That was it. I was dumbfounded. I lost the gamble. But then

he continued, "not until you return the visitor log so I can record the pass number."

I immediately passed him back the clipboard and took the pass and thanked him.

"Don't forget to hand it back to us before you leave."

"I won't!" I exclaimed and ran towards and through the security barrier with my laptop, papers and my new "access to all Derek's areas" pass.

Part Four - Finding Room 123

I was in. Well, as far as getting past the main security anyway. Now to find Room 123 which itself shouldn't be too hard.

Assuming the numbering system ran in a logical order, I could safely say that Room 123 was on the first floor, so I climbed the first flight of stairs and found that all rooms on this floor began with 1.

Heh heh! Easy game! By looking on the little signs on the walls that gave directions to the different rooms, I could see that rooms 120 to 135 were through a corridor beyond an electronically locked door that was opened by a card swipe machine. This was just past the tea room. I tried the door - it was definitely locked, so I popped into the tea room to decide my next plan of action and get myself a cup of tea from the tea machine. It was free, after all! I took a sip and then realized why it was free!! It was bloody awful. I returned back to the locked door with my belongings and cup of the barely-bloody-drinkable and was lucky enough to get there just as somebody was walking through it, so I hurried to tailgate, but the very polite gentleman looked to see me rushing with my hands full that he kept hold of the door for me. Human nature can be a beautiful thing!

I thanked him and found myself in a secure area of the building, so I walked through the corridor behind the gentleman and found Room 123.

Brilliant!

I opened the door, entered the room, and closed the door behind me.

Part Five – Finding the Envelope Stuck Under a Desk

I found the envelope that I was after; it was taped under a desk.

Conclusion

So there you have it. With just a bit of friendly chit-chat with the girl, the receptionist, and the security guard, I managed to fulfill my goal and come away with the envelope that I returned to my challenger. And why did I do the things I did to achieve this?

Well, that is another story, one that could last a lifetime. Social engineering is one of those massive subjects which is better described and taught by people who know more than me, such as people like Kevin Mitnick, who, in my regards, is one of the masters in this field. But to make a start and to keep it short, heed these pointers:

1. *Suit*. Always dress well, or to at least fit in with the crowd. You need to be part of it to blend in.

2. *Laptop/papers*. These give the impression of importance. Always good in an office environment, especially if you are rushing somewhere. Another good thing would be to go in with a police officer - even the security guards would bow to a higher authority. Saying that, my policeman friend was on duty so couldn't help me out. I do have another friend who is a stripper with a policeman's uniform, but I'd be worried about him stripping in the office before oiling up.

3. *The "stakeout."* Always good for seeing what people are up to at certain times of the day and the kind of people these are and their behaviors.

4. *The "forgotten" lighter.* This is one of my favorite techniques. You manage to get talking and, using the right words, someone can disclose a lot of info about the company that could be used.

5. *The empty cup*. A prop used to make it look like I've just come out of the building for a smoke. I'm part of the scenery, remember!

So there you have it. Another quick insight into my life. Don't try any of the above at home (well, elsewhere). Only try them if you have been legally asked to do so and have permission.

Now go celebrate by having a beer. Unless you are a kid, in which case have a glass of cocoa!

Enjoy yourself and be safe.

The Hacker Perspective

by Brainwaste

I have always been a hacker. Best of all, I have always been aware of it. I have always been able to push the envelope, to think outside of the box. I always chased the white rabbit and wanted to find out just how deep the rabbit hole went. Exploring and experimenting with everything has always been my way of life and I want to tell you all about it. Back in the 1960s and 70s, my family had a summer home in a community on an island off the southern shore of Long Island here in New York and it was here that I developed the hacker mentality and then put it to good use.

Being a hacker is not about doing certain things. It is about having a mind, and mindset, which allows one to be *able* to do certain things. It means to have an inquisitive mind which asks certain questions, finding the answers to those questions, and then following the leads to those places where the answers take you. To be a hacker means to look at things in a way that the average person does not know how to do or would not think of doing. Further, being a hacker is the best way to protect yourself in a world that is designed to dumb you down. Hacking opened my mind and made me examine and challenge the assumptions that I had taken at face value for the truth. Having an inquisitive open mind is the best defense against ignorance. Hacking was how I learned that the system in place was here to dumb me down and make me/keep me a sheep. This was the purpose of the status quo.

I have always been interested in acquiring what others deemed to be "forbidden knowledge" and learning about things that others told me I should not be knowing. My thirst for subversive knowledge grew daily. Unfortunately, *2600 Magazine* did not exist at this point in time. One summer day, I found Abbie Hoffman's *Steal This Book* while browsing at the local bookstore. Hoffman's book inspired me to pursue my own mischief and gave me plenty of ideas of how to do so. Hoffman's book pointed me in the right direction to learn what I wanted to learn and explore things that I wanted to explore, just like *2600 Magazine* does for me today! Hoffman opened my eyes to the fact that there were many others in the world who saw things the way I did and who also thought like I did.

The first hack that I did was easy, fun, and profitable. My friends and I used to always play pinball at the local diner which had several machines. Our favorite machine was called Doodlebug. One of the main objectives of the Doodlebug pinball machine was to score points by making the machine "doodle." To make the machine "doodle" was to make a steel pinball that was located under the inner surface of the machine go up and down in the vertical tube that contained it. This action of "doodling" was initiated by hitting certain lit targets in a specific order. When the machine was in this mode, the player would earn points in an accelerated manner and thus would be able to win extra balls and free games if enough points were scored. Getting things for free was very important to me as money was always tight.

I needed to find a very easy way to make the machine doodle so as to rack up enough points to get plenty of free games. I remembered that when I went into the shed that we had in the back of our house to fetch something, I saw a very large magnet which looked very powerful. The seed had been planted in my mind to look for a way to hack the Doodlebug pinball machine for free games. So the next time I was playing the Doodlebug machine, I had my trusty magnet with me. Within a short time of playing, I hit the lit targets in the proper sequence and had the machine doodling 100 points every time that the encased steel ball hit the upper and then the lower bumper in the tube that it was in. When I saw that the machine was about to stop doodling, as there was a set time by the machine on this action, I made my move. As fast as possible, I placed the magnet on the glass top of the machine, directly over the tube where the steel ball was quickly scoring points. The force of the magnet was powerful enough to keep the steel ball bouncing back and forth between the bumpers and keep scoring enough points to earn some free games for me. I held the magnet in place until I had 15

free games. Fifteen was enough for me. No sense in being greedy.

One day a friend of mine, who I will identify only as X, stole a lineman's handset from a telephone company repair truck. X told me that the lineman's handset was an item restricted only to authorized phone company technicians and was a very hard piece of telephony to get your hands on. X told me that this was a device used by telephone company repairmen to connect to a phone line for testing purposes. X told me that there were many interesting things that we could do with the lineman's handset, as using it was just like being an extension on that phone line. This concept just blew my mind and I couldn't wait to experiment with the lineman's handset.

X and I found a Telephone Network Interface (TNI) outside of a building. X opened up the TNI with a screwdriver and attached the headset's pair of alligator clips to the terminal wires. We got a dial tone and were now ready to play with the PSTN. X made sure that the ringer was turned off so that an incoming call would not draw attention to our activities. Wiretapping was first on our agenda. X and I took turns attaching the headset's alligator clips to different sets of terminal wires until we found a phone line with conversation on it. After testing a few lines, we were successful and eavesdropped on a couple making plans for a party at their house that weekend, a restaurant owner ordering liquor and food from a supplier, and someone discussing the hot date that he had the previous night. Next, we made some free, and untraceable, phone calls. X made some local calls to some friends and I made a long distance call to my cousin who was on vacation in Italy. The best feature of beige boxing was the ability to make calls and charge them to any number that we liked. There was one specific individual in our town who irritated me. I saw this as a perfect opportunity to exact my revenge. Without getting too detailed, this individual found long distance charges on his next phone bill that amounted to just about two thousand dollars.

Our town was not without its share of social problems. Most of these problems that my friends and I encountered were with the repressive Suffolk County Police that patrolled our community. The cops always enjoyed giving people a hard time for some petty violation of a village ordinance, either a real violation or one that a cop either exaggerated or simply made up just to fuck with you. One hot summer afternoon, I was walking through the central part of our town eating a slice of pizza and holding an open can of soda in one hand. As I passed the village green, someone yelled "Hey you!" I looked around, but did not see anyone. "Yeah. You wearing the Yankee cap. Over here." I turned around and behind me was a uniformed Suffolk County cop. "Come over here," the officer commanded. "Right over here in front of my patrol car. Walk over real slow." I obeyed these orders, not knowing what law I had broken to deserve this treatment. "Don't you know that it's a violation of the laws of this incorporated village to eat any food or have a drink or open can of any soda within the limits of the central township?" "You're kidding me? Right?" I replied. "Drop that food and drink right now!" the cop commanded. I obeyed. "Turn around and put both hands on the hood of the patrol car. I want to see ten fingers on the fender. Come on. What are you waiting for? An engraved invitation?" I placed both my open hands on the hood of the patrol car and the officer frisked me.

"Turn around and face me," he ordered. Again I obeyed. "Since I didn't find any weapons or other contraband on you, I'm just going to write you up a summons for having food and drink in a part of town where possession of food and drink is prohibited." "But what specific law did I break, Officer? Give me a citation," I protested. "I have no citation to give you. You broke a Say-So law." "What is a Say-So law?" I asked. "You broke the law because I say so." This was the response of Suffolk County's Finest. And with that, he wrote up a summons for a violation of some obscure village ordinance with a $250 fine. This is what is called an "attitude arrest." This is done when a police officer does not like someone's attitude or behavior. It shouldn't happen by itself, as arrests are legally authorized only on "probable cause," when an officer has reason to believe a criminal offense has been committed. When a cop did something like this (a police action which lacks any logic), we called it "mind over matter" as in "They don't mind and you don't matter."

One day, I went to the local Suffolk County police station to file a complaint against someone (no, not the cop who ticketed me). I went over to the desk sergeant on duty and he told me to take a seat on a nearby bench. From my view on the bench, I could see into the offices in the back of the station, where high level Suffolk County Police personnel worked. The Chief of Police of our town also had his office in this area. I thought about the type of work that those people do and what sensitive information might be in the files of the cases that they were working on. If I could get into those offices and check into the papers that those case files contained, I would be in a position to know what was really happening in

our community with regard to police matters. So I waited to file my complaint and I also waited for an opening to come along where I could get into those offices and run through the files. After about 20 minutes of waiting, the desk sergeant told me that he had to leave on an assignment and that I should just "sit tight" and wait for someone to help me file my complaint. After the sergeant left the station, I made my move and slid into the back room offices without being seen. After a cursory look around, I found the desk where the Chief of Police worked. The Holy Grail. There were some files on the desk that the Chief had obviously been working on and I opened a few up and eagerly started reading.

One file detailed traffic ticket numbers and another some summarized reports of vandalism. Nothing spectacular. The next file I read was very interesting indeed. It detailed the orders from Suffolk County Police Headquarters to the Chief of Police of my town to cover up a local scandal in our town that the cops were investigating. The Chief was ordered by Suffolk County HQ to withhold any specifics of the scandal from the public and to our local newspaper as well as any other media that inquired about the scandal. When put on the spot and pressured for answers, the Chief was ordered to lie when questioned and to mislead the public and press by putting out a fraudulent cover story as to what the scandal was about and as to what their investigation had found out and where it was heading. The reasoning behind this dishonesty and censorship on the part of the Suffolk County Police was this: not to make the public uncomfortable, even if that means diluting, sensationalizing, or lying about the truth.

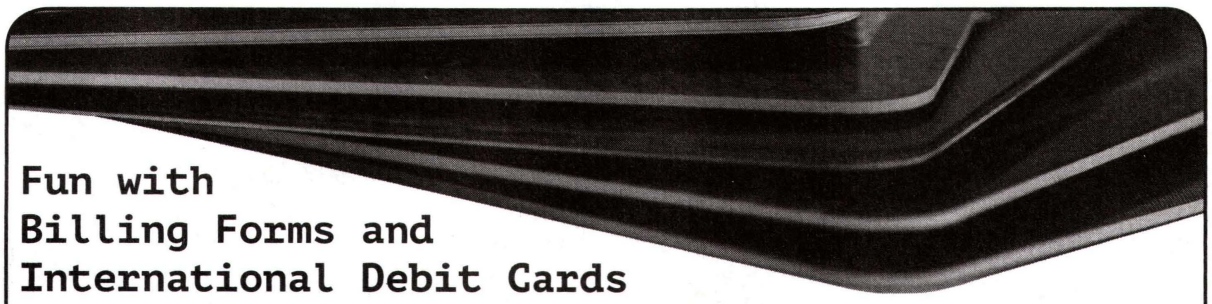
The Suffolk County Police distinguished two categories of arrest and imprisonment: one for breaking a law, the other for political reasons. The difference is clear: Someone who spoke out in public against the policies of the town's mayor is considered a different type of criminal than an armed robber who knocked over the town bank. One is an "everyday lawbreaker," while the other is a threat to the political hegemony of the establishment. The authorities in our town always hated me because I was for real. Many people do a lot of heavy talking, but when it comes down to the point of action, they disappear. If someone was the victim of any type of injustice, I would always turn up at their side fighting for them. I have always had a huge problem with authority and these experiences only made it worse.

Although many of the hacking activities that my friends and I did back in those days were illegal, I did not then and do not now believe anything that we did do was wrong. Our actions were not evil. Nobody actually was hurt by what we did. I never acted in a malicious way. I only wanted to experiment, explore, and learn. Expanding my horizons and obtaining knowledge were my goals. There is a distinction in the law between actions that are *malum in se* (evil in and of itself) and actions that are *malum prohibitum* (wrong only because of the existence of a law prohibiting it). An example of *malum in se* would be murder. In every society, such a thing would be recognized as wrong. It would require no act of the legislature forbidding it to inform people that it was wrong. An example of *malum prohibitum,* on the other hand, would be the statute prohibiting driving through a stop sign without coming to a halt. Absent such a law, to do so would be a morally indifferent act. In the case of hacking, there is a point beyond which I will not go, and that is anything my conscience tells me is *malum in se* or that my judgment tells me is irrational. I have no problem with doing something that is *malum prohibitum*. I will (and have in the past) hacked something after satisfying myself that a) it was a legitimate way to learn about the system; b) a question of *malum prohibitum;* and c) a rational action.

British author George Orwell wrote, "Freedom is the freedom to say that two plus two equals four"- even though you're being told otherwise. It's the freedom to give voice to the *real* truth, untainted by disinformation and propaganda. Is that freedom of value to you? You have a choice. You can continue to believe what you've been told, or you can open your eyes to examine the facts and discover the truth for yourself. Hacking is your ticket to this freedom. If, at the end of your journey, you conclude that you had previously been manipulated and deceived, you may find yourself asking what other "truths" may be illusory. How accurate and objective is other information being fed to us? Have courage. There are many uncharted roads ahead, much to be explored, and a flock in the meadow in need of brave shepherds.

Brainwaste is an open-minded, dedicated computer hacker and phone phreaker who is always experimenting with technology. His goals in life are learning, questioning authority, and hacking everything.

HACKER PERSPECTIVE submissions are closed for now.
We will open them again in the future so have your submission ready!



Fun with Billing Forms and International Debit Cards

by musashi42

Disclaimer: all of the below is for educational purposes and to help when it comes to online payments (of digital goods/bills) which, due to silly formalities, can't be processed if you have a debit card without a U.S. billing address.

The important thing to know when it comes to website related hacking is how the sites work and the code behind them (which goes for everything). Knowing PHP and MySQL made this quite an interesting thought experiment mixed with the practical approach. It was more of a traditional meaning of the word (i.e., forcing a system to do what it's not supposed to do). I wouldn't have discovered this if I had a debit card that had a U.S. based billing address (and a lot of money), but I had the one that doesn't and I really didn't want to lose cash on withdrawing the money from the ATM in order to pay my bill and, sadly, the payment form's billing area doesn't have the country dropdown, so I had to think back to my own coding of forms, databases, and tables to see if there was a way around it.

This is where the true insane fun begins. The typical online payment form consists of the following fields: Card Number, Expiration Details, and Name/CVV. Then there's the address listed and checked with a radio button that matches the address where the service is installed, but next to it there's an option to enter a different address. The different address has the usual fields and none of them have a dropdown button. So, I simply assumed that certain fields weren't being validated (years of having fun and sometimes profiting from XSS discovery/fixing taught me a lot about what fields are less likely to be validated) and the most obvious field in this case was the address field because there are so many addresses (and it was a very lame looking website system, which is odd considering they are a pretty huge and very hated company) that it allowed for entering anything as a billing address in order to match with the billing address listed on my debit card's issuer website (and it can't be edited there, hence why I have to go through these hoops). I've also learned from this exercise that my debit card's issuer isn't taking State and Country fields into consideration when it comes to validating the billing details.

There are additional requirement for this to work and this is rather simple when it comes to the United States. It involves finding the state in the U.S. which has the city with the same name as the city from whatever country you are from. Basically: Paris, France equals Paris, TX; London, UK equals London, MI; Berlin, Germany equals Berlin, OH, and so on - you get the picture. The zip code on this particular website's online payment system was also lacking validation (I wasn't sure if my debit card's issuer would proceed with the payment if it didn't have a matching zip code, but I didn't test it further in order to avoid them noticing that someone was messing around). I tried the same technique for another website (also involving paying the bill) and that website didn't accept the address. But then again, if a GPS device has a database of all of the addresses, or at least most of the addresses, then why wouldn't the same go for the website in question, especially one whose owner/company is extremely rich and equally hated (yes, I'm paying hard earned money to two hated companies - oh well).

I didn't try any reflective XSS attacks because, well, it might have ended up as a stored one and I don't want to shit where I eat, so to speak (and they don't have bug bounty), and considering that they still get the money, I can't classify the billing exploit as a bad thing. However, I'll probably try this technique on other websites where they are asking for the United States-based address when I want to buy a digital product and avoid losing money by buying a gift debit card.

GOING NUCLEAR - A TALE OF REVENGE

by 2dedd54f25ae2730225e
➥6f1b8968fda52f0831ce

It all started when my wife posted an article to social media about taking care of handicapped family members. She has a severely handicapped family member, so she naturally has a soft spot for people in that situation. After posting the article, a person neither of us know commented on the story making fun of handicapped people. My wife, unacquainted with the cruelty that's common on the Internet, responded by asking the commenter how they could make fun of a disabled person when they themselves could have easily received the same lot. This is where things heated up. The commenter proceeded to be even *more* aggressive and insulting about the disabled and towards my wife personally.

After the second encounter, I walked into the room and found my wife crying. She showed me what happened and I, understandably, began to get angry. I reached out to the man privately to tell him that his jests had, in fact, brought my wife to tears and asked him to lay off. I naively thought that he would see that his trolling had gone too far. His response took me by surprise. He scoffed and threatened to do far worse to her and me.

I understand that this was just one of a million social media wars that erupt every day and that this complete stranger posed no real threat to my family or myself. I will not try to justify the actions I took immediately following the encounter. When he threatened my wife and me, a switch flipped inside of me and I intended on burning this fool like he'd never been burned in his life. I loaded a live Linux distro (Tails) from an SD card, fired up Tor, and began building a basic profile. I searched through social media, reverse email lookups, and various other places until I had more than enough information to execute a nuclear strike. I found a sex offender registry and navigated to one of the more scary and local profile pages, and copied the HTML of the page down locally. I stripped out analytics, moved the CSS to the head of the document, and replaced the sex offenders' image and name with the image and name of my target. The single file HTML document worked as expected on my machine. Now to get it online.

At this point, the only assets I had to deal with were an image and an HTML page. I dropped the image into an anonymous image host (there's plenty) and edited the HTML to point to that location for the profile picture. Next, I knew of a pastebin-like service that let you paste HTML and the service would serve up the page just like a web page. This particular service no longer exists, but the same thing can be accomplished with a temporary Dropbox account if a suitable pastebin can't be found.

Next, and this is key, I purchased a domain that included the name of the sex offender website with the addition of "-alert" at the end. ICANN requires that a real identity be connected to a domain name, but this can be circumvented by using a domain name proxy service, fake personal information, and a burner email. I needed a registrar that had this loophole and accepted Bitcoin. It didn't take me long to find one. After purchasing the domain, I set it to forward to my pastebin page with domain name masking turned on (this would ensure that my domain showed as the URL). Lastly, I double-checked to make sure all the links on my pages linked properly to the real sex offender site to advance the allusion that the page was a part of that website.

The table was set. It was time for the main dish. I looked around online and found a flyer designed to inform neighbors when a violent sex offender moves into a neighborhood. I modified the flyer, adding the target's image, personal information, and the URL to my fake web page. I knew the target's home address and place of work from the profile I initially compiled. I sent the PDF to a printing/shipping service that accepted Bitcoin under the guise of representing a neighborhood watch and had the flyers sent to the target's neighbors and place of work. Like I said, I don't encourage this kind of reckless behavior.

This entire attack took me an afternoon and cost less than $30. Everything was wiped after the operation ended. The Bitcoin wallet, the burner email, and local media were all destroyed when I pulled the SD card. I never sought to follow up on what kind of fallout ensued. Even if and when the entire ordeal was cleared up on my target's end, I suspect that his neighbors and associates would forever judge him with a measure of suspicion.

It's good to take mental notes of services that accept Bitcoin with the idea that they can frequently be piped together to accomplish unusual things. If nothing else, the above course of events illustrates the brave new world that hyper connectivity and anonymous cryptocurrencies have made possible.

Don't be evil!

INFORMATION SECURITY– YOU ARE THE KEY

Basic Rules of Information Security:

1. **Restrict data access to authorized users.**
   - Access only information necessary to perform tax administration duties.
   - Follow Unauthorized Access (UNAX) guidelines and procedures.
   - Never access information in which you have a personal or financial interest.
2. **Recognize and protect sensitive information.**
   - Lock up sensitive reports and computer media containing sensitive information when you leave your work area.
   - Shred printed reports containing sensitive information when they are no longer needed.
   - Diskettes and CDs containing sensitive information that are no longer needed should be given to your manager to ensure proper destruction.
   - Be aware of and challenge unauthorized persons in your work area.
   - Be aware of the visibility of information on your workstation display screen.
3. **Protect your password from misuse and improper disclosure.**
   - Keep your password confidential - Don't share your password with anyone.
   - Never write down your password and post near workstation.
   - Change your password if you feel it has been compromised.
   - Best passwords contain a complex combination of letters, numbers, special characters and at least eight characters in length.
4. **Protect your workstation.**
   - Log off of or exit any applications (sign-off IDRS).
   - Log off/lock your workstation (but do not power-down).
   - Secure laptops in lockable containers.
   - Do not move equipment or exchange system components without authorization by Information Technology Services (ITS).
5. **Comply with the IRS electronic communication requirements.**
   - Only e-mail SBU or taxpayer information with encryption capability.
   - Only e-mail SBU information inside the IRS network.
   - Ensure anti-virus software is current.
   - Do not forward chain letters or unsubstantiated warnings (like virus hoaxes).
   - Personal use of IRS ADP equipment must not result in loss of productivity or interference with offical duties.
   - Do not download, use or install illegal software (including games and screen savers).
   - Do not open attachments from people you don't know.
6. **Back up information and store securely.**
   - Protect diskettes and computer equipment from physical hazards.
   - Make backups regularly.
   - Store backups in a separate location from the original.
   - Label all diskettes and other computer media.
7. **Use only legal copies of proprietary software.**
   - Know and obey federal laws and licensing restrictions.
   - Do not make or use illegal duplicates of proprietary software.

Apparently this document is still being passed around internally at the IRS. We particularly enjoyed the THREE references to diskettes and we sincerely believe they still use those over there. It's also fun to note that screen savers are illegal software by default.

MALWARE ATTACKS - LEAVE THOSE [Banks] ALONE

by lg0p89

First, all apologies to the Pink Floyd fans for modifying the noted lyric.

Bank breaches have been in the news with an increased frequency lately. The banks tend to be a good target for the deviants and their respective malware for two primary reasons. First, this is where the cash is located, and a lot of it. This can be transferred out with some ease, dependent on the system and structuring of the transfers. This is also where the client's information is in a digital and downloadable format. This includes all of the information that can be sold to other parties for their own nefarious uses.

Unfortunately for everyone, the bank clients are becoming numb and apathetic to information security. They have been inundated, from their perspective, with having to change their passwords too often (in their own view), the breaches and thefts in the news, and emails telling them their computer is infected (be it infected or not). In this day and age, it would seem to be intuitive for the bank's clients to be hyper-vigilant, especially with the potential for loss to them. The Help Desk and bank, however, still is receiving complaints regarding security, ranging from having to change their password for the ATM too often, sending personal documents with their private information (i.e., tax returns, W-2s, etc.) securely, and being asked for state or federal issued identification or other identifying information to verify the person's identity, and everything in between.

Previous Banking Malware

Banks as a target have not and probably won't change in the future. As noted, the banks have what the criminals want. Within the last couple of years, the Zeus malware was in the news. This also was directed at the banks and their clients. Zeus did quite a bit of damage to the affected banks. Also, banks have had the pleasure of feeling the negative effects of the Gameover malware, which was shut down back in June of 2014.

Shylock's demise recently made the headlines. This has been operating since approximately 2011. This case of malware received its name due to quotes from Shakespeare's *Merchant of Venice* being in its code. This is also known as Caphaw. The coding for this was rather inventive and sophisticated. These coders are believed to be located outside of the U.K. and first targeted the U.K. computers and banks' clients, and later widened their target base to banks in Germany, Turkey, Italy, and Denmark. Of the targeted banks, three quarters were British.

Modus Operandi

With this malware, the coders learned from the prior generations. Generally building on past experiences is a good thing, except with this incident there is a malware application involved. This did, however, use much of the same methods as the other significant malware occurrences.

The malware can be spread via spam. Here, the user clicks on the link that appears to be fine from their view, and their system becomes infected. Shylock waits patiently in the background as the user continues to go about their business on the Internet, looking at news stories and different products to buy. When the user eventually logs onto their bank's website, the malware may either display a false website, which appears to be perfectly legitimate (man-in-the-middle usage) or key logs the user's system. As an alternative, the malware may also utilize screen shots to gather the information it wants. The user's credentials for the bank are then captured and sent to the command and control center. This may then be used or sold abroad in the dark web.

This sounds very basic and much like any other malware that is present. There is, however, a new aspect to this in that the malware is rather dynamic and not static. This was not released into the wild in one format and allowed to run rampant through users' compromised systems, but developed over time. This began with the basic code for the malware. This later incorporated other aspects, e.g. Skype's chat function, into the attack. It was written to be of a somewhat modular design and incorporated certain aspects of the malware when wanted. This is

somewhat like ordering from the restaurant what you would like with your steak.

Shut Down

For obvious reasons, this caught the attention of law enforcement. The task force, led by the National Crime Agency, a U.K. law enforcement agency, and involving the FBI, Europol, German Federal Police (BKA), and several infosec firms, searched for information on the malware and its infrastructure. Due to their efforts, Shylock's infrastructure was found and shut down. This was done via the task force eventually finding and seizing the command and control servers and domains. These were used by Shylock to communicate with and control the infected computers.

Malware attacking banks and their clients is not going to slow down any time soon. The rewards (e.g. cash, personal identifying information, etc.) far outweigh the risks. The malware has shown itself to adhere to a simple trend. This will continue to become more advanced and allow for the utilization of different forms. This will continue to make it more difficult to find and later quarantine the malware. The potential losses to the banking system continue to be massive. To fight this, a layered approach and different agencies have to be involved. Each of these brings a slightly different viewpoint and method of working. With these entities working together, the threat is removed long before it would be with the agencies working alone.

Malware is, unfortunately, all around us. It can come from email sent to people by strangers. It can come from visiting different websites. Each of these instances may include another version of malware. There used to be a limited number of coders who were talented enough to write effective malware. With the wiser use and understanding of the Internet, computers, and additional training, this skill has grown exponentially. The coders are always looking for different malware to write to affect different users.

Tinba

Tinba is also known as Zusy. The name came from a shortening of Tiny Banker. This example of malware is very small, only taking up 20k. Although the size is small, this is still very useful and functional for the criminal aspect, and works as good as other malware that is much larger. This was written to steal bank login credentials, credit card numbers, financial information, and other data. Tinba can also be modified and customized.

This was discovered in mid 2012. At that point, more than 60,000 computers in Turkey were infected. The source code was published. Initially, it appeared to have been a bonus for law enforcement. After all, the appropriate law endorsement agencies would know what to scan for. Once you know the specifics of the target malware, this should then be easier to track. This actually meant, however, that others would be using the malware with more regularity and spreading the known version of the malware, along with the modified versions. This made the tracking and enforcement more difficult.

This was also seen previously with the Zeus malware. With this, however, the source code was leaked in 2011. Once this occurred, Zeus' use by the criminal element increased significantly.

Deconstructed

Tinba was written to steal data from consumers visiting their bank's website. This was coded to use a "man-in-the-browser" (MitB) attack. This works by injecting code into the browser, which changes the bank's website and content. The modified browser may take the form of additional fields in the bank's website. These additional fields are required to be completed prior to moving to the next site.

This also places the malware in the user's system. The infected system can also be set up to be used as a botnet. A later version of Tinba made changes to the user's interface.

Pertinence

The banks and their clients continue to be targeted by malware. As mentioned, this will not slow down and will grow indefinitely. Tinba likewise followed this route via targeting online banking. At first, this was focused on banks in Turkey, and eventually expanded its target market and range.

Tinba provided yet another tool for the criminals to use. The modification and later versions are useful but have a tendency to make it more difficult to track. As this is the case, this piece of malware will continue to be important and something to watch for.

CONCEPTIONS

Furthermore

Dear *2600:*

Hey, folks! I've flipped through tons of your issues at my local hacker cafe. It's always an amazing read. I should go find some room in my college student budget to subscribe to you.

In your Autumn 2014 issue, I read "The Demoscene - Code, Graphics, and Music Hacking." It's fantastically interesting stuff. It just occurred to me that I hadn't seen anything about live hacking, though. Live hacking is demoscene performed live, with the source displayed to the audience. Its community is a little sparse and quiet, but there's a lot of interesting footage of live hacking events. Live hacking is often limited to audio at algorave events, but there are tons of suites that also focus on visuals - some even work with VR headsets.

Tidal is one popular live hacking mini-language. It's built on top of Haskell and specializes in manipulating audio patterns. This language, along with many others, is live-interpreted: hit a few bound keys and the changes you make are instantly applied to the pattern. Gibber is another clever project: it manipulates both audio and visual patterns in-browser. There are loads of clever hacks that make it efficient enough to run smoothly: I've hardly seen such an intensive JavaScript project that looks so silky smooth. There's a speech from the author of the project which explains its processing wizardry in more detail, presented with a bonus live performance at http://toplap.org/, which is sort of the community center of the live hacking scene. There are loads of performances to watch there, and tons of information for anyone who takes an interest in this culture. I'd encourage any amateur coders and demoscene fans to poke around there - come join the live scene!

nfd9001

Thanks for the window into yet another truly fascinating culture.

Dear *2600:*

The past few issues of the quarterly had some interesting articles from the perspective of a missile officer.

While the chances of a civilian visiting an active missile facility is probably slim to nil, visiting a deactivated site is possible. Growing up in western South Dakota, Minuteman missile sites were a common sight while traveling the rural highways.

The missiles have been gone for over 20 years, but there is a launch site and a control site that are now open to the public and part of the National Parks System. It was preserved as much as possible to be as it was in the "Old War" area.

The Minuteman Missile National Historic Site consists of three separate parts: a visitor center, a launch control center, and an actual launch site. Currently, there are no fees at this historic site. There is some discussion about fees for the tour of the launch control facility in the future, though.

This past summer, my sister and niece were back home visiting. After a drive through the Badlands, we stopped at the visitor center to see if a launch center tour was possible. The tickets for the launch control center were all taken for the next tour, since they are available on a first-come, first-served basis. The tours are limited to six people due to the small size of the launch control facility's elevator. Not wanting to wait for the next tour, we decided to see the actual launch site. The launch site is a self-guided tour. You park your vehicle in the parking lot and enter through the gate. There is a "skylight" over the missile silo and a deactivated missile sitting in the silo.

Visitors to the site can look down into the launch silo and walk about the launch site. There is a phone number posted on a sign at the missile launch site. You dial it using your cell phone and it gives you a guided tour using touch-tone prompts. Just don't whistle into your phone while touring the site, as we all know what might happen when whistling into a telephone....

Here is the phone number and prompts: 605-301-3006

1) *Missile Plains*
2) *Why South Dakota*
3) *Missile Launch*
4) *Missile*
5) *Ultra High Frequency Antenna*
6) *Soft Support Building*
7) *Maintenance Access Hatch*
8) *Security System*
9) *Putting in a Missile*
10) *Minuteman Missile, Past, Present, Future*

Most, if not all, of the former facilities have been returned over to the original land owners, and there are restrictions on what can be done with the property. One is not being able to dig down more than a few feet.

Most, if not all, of the former launch sites still have the perimeter fences. Some are being used by the land owners in interesting ways. Some have hay bales inside, my guess is to prevent deer and cattle from eating the supply of hay. Another use I have seen is a beekeeper who has placed their beehives in the fenced in area.

Located just outside the main gate at Ellsworth Air Force Base is the South Dakota Air and Space

Museum. A Minuteman II exhibit is on display there. Also, a base tour is available for a nominal fee. A missile training site is on the tour. I was able to see the inside of the training site several years ago when the base had an open house/air show.

Here are several sites to look up: http://www.nps.gov/mimi/index.htm, http://www.sdairandspacemuseum.com/exhibits, and http://www.silo-world.net/.

Brian from South Dakota

This is indeed interesting stuff - thanks for sharing. We also found it extraordinarily cool to be able to take this tour remotely and we wonder how many other such services exist that can be tied into from around the world.

Dear *2600:*

Thank you for your amazing work on my Hacker Perspective. You captured exactly what I was going for, while presenting it in a vastly less Internet blur of text. I have become slightly better at wording my dialog, but the skill of the *2600* editors should not go unsung.

I really enjoyed the buildup tone that matched the original blur of words I sent in. I am pretty impressed to see the shorthand personal notes I submitted read so coherently. Respect to everyone who reads the emails and answers the phones, as well as readers, writers, and that random person who asks a good question. Bonus Shout: The Piano Guy's "Attitude Adjustment: How to Keep Your Job" (32:2) article was excellent. If only more persons respected the fact that others do different things. One person's skill is another person's presumed constant.

Pic0o

We appreciate the acknowledgment, but the content came from you so don't forget to give yourself the credit you're due. We often have to do a degree of editing to make an article or column work and it's great when people understand what goes into that process. We hope those of you out there who think your words won't pass muster will take that into account and send us what you come up with regardless. If you have something truly interesting to say, it's our job to make sure it reads well.

Dear *2600:*

Thank you for publishing my article "Abusing the Past" and the back cover photo, too!

I had a rush of inspiration, and wrote ten tips to becoming a hacker. These are right out of my personal experience:

1) Get it into your mind. Hacker means ethics. Hacker means curiosity. Hacker means a desire to improve things. Hacking is fun. And healthy. As I usually say in my talks: "Do any of you drive a car? Do any of you drive *really well?* Oh, so I guess you are probably a killer." Oh, so you are good with the computer. That means you are a criminal, right? Get it straight. Any person can become a criminal. It is not hard. You just need to be a bad person. You can blame any other bunch of factors but in the end, it means you are evil. Mistakes, that is something else. And you will make many growing up. And then some. With or without the computer knowledge.

2) You will need to open up. You can use any OS to do lots of things, but the more multi-platform knowledge you gain, the better. Use Windows. Use Linux. Use more than one OS. This is far easier to do today. Between your game console, your computer, and your tablet/smartphone, you already have two-plus OSes, surely.

3) Break things. Break yourself, too. Pursue a different area of knowledge, a different interest, such as music playing, literature, languages. Try new stuff. Enjoy the experience.

4) Love those around you. That means respect, too. You will make it easy for them to support your interests, especially growing up.

5) Find a team to share knowledge with. I suggest a *2600* meeting. You will find what areas of IT knowledge most interest you this way, too. For instance, I love defense, forensics, and all things networking/comms, especially authentication and data sharing/analysis. But I get bored with the offensive side of things.

6) Programming is a must. Stick to a limited number of languages at first. I would suggest Python, C, assembler, and some C# (it is quite an awesome language from which you will learn a lot). Try to attack your code. Debug as crazy. Attempt to understand why stuff breaks. In 1998, I coded a multiuser BBS for Linux in plain C. It was the way to understand all things about Linux, as I had to learn IPC, sockets, processes, input handling, locks, filesystem, terminal capabilities, session control, etc., etc. Making it crash and debugging it allowed me to understand how an exploit would work. Learning how to code an exploit is also extremely useful, as it gives you the "other way round" knowledge of operating systems and code execution.

7) Help others. I cannot emphasize this enough: your experience and your knowledge have no value if you do not find a way to help others, in any way, using any methodology. Be loyal.

8) Do not allow yourself to be used by evil people. Information gathering, one of the stages of "how to attack a problem," can be applied socially. Avoid bad actors. But you will find yourself that the concept of "know your enemy" is also valuable. Remember I mentioned ethics?

9) Get out in the open. Analyze your surroundings. Travel. Technology is everywhere, but subtlety is beautiful. Balance.

10) You will one day die. Try to make the best out of life. Think about what you will leave behind. That is the real, the ultimate hack.

Hugs to everyone out there.

Buanzo
Argentina

These are all extremely good points and we appreciate your putting them together. We do want to add, however, that even this broad view of hacking

doesn't cover it all. Programming, for instance, is vital in certain areas, but it's not essential for a hacker to be a programmer. What is needed is for the curiosity and determination to be present. Hackers have existed since long before computers came about and they can be found in places where there is no technology at all. Computers, programming, etc. lend themselves to hackers because of the possibilities for endless exploration and innovation. But those elements also exist in other realms in a more subtle way. It's all incredibly inspiring.

Dear *2600:*

I was a student at a small private college, graduating in 1957. I learned from someone that a 2k resistor grounded to the overhead light socket and to the line of the removed voice box in the receiver caused the telephone dial tone to trip on (for local calls). This worked for the last two years of school. Girls from Skidmore and Russell Sage called me on long distance (and the folks from New York City). Afterwards, in the military, I didn't need it as I had access to call anywhere.

Edson+

Now surely you can expand that story a bit and tell us more about the phone system back then, along with any other bits of technology and trivia that hackers might be interested in. Please send your stories to articles@2600.com. Our mailbox awaits.

Dear *2600:*

In her book *Travels with Myself and Another,* journalist and war correspondent Martha Gellhorn visits Nadezhda Mandelstam, widow of the poet Osip Mandelstam, who was purged by Stalin. At a secretive dinner in Moscow, Gelhorn relates, "A man said, 'You know how to fix the phone so is safe? No? Come, I show.' The man pushed the dial all the way round and locked it in place with a pencil. 'That way they do not hear what you are saying,' he said. 'Also a cushion over is good,' said Mrs. M. I have never been able to do it since so cannot have seen right." What was it that Gellhorn could not replicate? How did unlocking the phone make it safe from the KGB?

Marco

Locking a rotary dial phone with a pencil can be tricky. That was probably the hardest part of the operation. We have no idea whether such a trick had any effect on old Soviet phones, but we can't say it's impossible. Most likely, this is just another urban legend, like being able to dial a special phone number in the States to see if your phone was tapped (which makes absolutely no sense if you stop to think about it). The fact that they topped it off by putting a cushion over the phone tells us that even they didn't really believe the pencil was protecting them against eavesdropping. We would love to hear more such stories from that particular era and region.

Dear *2600:*

This is in response to Metalx1000's articles "Out of the Box Survival, Part One. A Guide to PowerShell Basics" (32:1) and Part Two (32:2). I was happy to see these two articles in *2600* as Windows system administrators know the benefits of PowerShell for automation and administration, but PowerShell is often overlooked by hackers.

In 2002, Microsoft was developing a product called "Microsoft Shell" that was created to overcome the limitations of the command line. Windows PowerShell was released in 2007 and Windows PowerShell 2.0 was fully integrated into Windows 7 and Windows Server 2008 and all Windows operating systems since. PowerShell borrows much from Linux including many Linux commands. With PowerShell capability, Windows becomes a more powerful hacking platform. But remember that PowerShell uses Microsoft's propriety source code. Since this is not open source code, PowerShell will not be as versatile a hacking tool as compared to Linux. But this demonstrates that Microsoft now understands the strengths and advantages of the command line. The terminal in Linux gives us complete control of the OS and PowerShell expands the capability of Windows in this regard. PowerShell has all of .NET at its disposal, which on a Windows machine is a very big deal.

Bash is mostly not worth comparing to PowerShell, because Bash is mostly text-based and not object-based. They operate differently (object passing vs. strings), but PowerShell (drawing on .NET) can achieve many tasks which Bash can perform. PowerShell can pipe meaningful objects as variables to a series of cmdlets (the pipeline), unlike Bash, where the output of any executable passes plain text to the next, which then has to be filtered for specific strings. For example, to kill a process in Bash, you will use something like: ps –ef | grep "chrome" | awk '{print $2} | xargs kill. In PowerShell, cmdlets spit out objects. So the above example of killing a process translates to: ps –name chrome | kill. PS and Kill are aliases for "Get-Process" and "Stop-Process" cmdlets.

PowerShell is perfect to use for attacks with a USB device called an HID or Human Interface Device. If we have physical access to a computer and wanted to hack into the system, what would we do? Now that most computers no longer allow AutoRun by default, we need to get creative. The HID looks just like a standard USB stick, but instead of storing files and data, it stores keystrokes. When plugged into a computer, the computer sees the USB stick as an HID. What does that mean? Simply, the computer thinks that the device is a keyboard. When this happens, the computer will run the PowerShell script loaded on the HID, since the computer has now been tricked into thinking that a human is typing in the commands on the keyboard. With a simple scripting language like PowerShell, you can craft client executable payloads capable

of changing system settings, opening back doors, retrieving data, and initiating reverse shells - all automated and executed in a matter of seconds. PowerShell scripted exploit payloads almost never trigger anti-virus as most executables do.

I am still learning about PowerShell: its features, functions and applications for hacking. If I discover more that is of interest to *2600* readers, perhaps I will write my own article on the subject.

Brainwaste

Dear *2600:*

In the Spring 2015 (32:1) issue, "nachash" wrote an interesting and informative article about hidden services ("So, You Want to Be a Darknet Drug Lord...."), including reference to extradition treaties (no countries mentioned) and the Mutual Legal Assistance Treaties (MLATs), and figuring out which countries don't provide legal assistance in extradition proceedings.

However, I feel the article could have been much more informative by naming the countries in alphabetical order that do *not* cooperate with the U.S.A. in extradition proceedings... North Korea being one of them - not that I would ever want to live there anyways!

For educational purposes, I am almost certain that the rest of your readers would also love knowing which countries do *not* cooperate with the U.S. in extradition proceedings, especially for those who do not have access to the Internet.

Nick

This is what we were able to find online, which may not be completely accurate, but should give you a good sense of what's out there: Afghanistan, Algeria, Andorra, Angola, Armenia, Bahrain, Bangladesh, Belarus, Bhutan, Bosnia and Herzegovina, Brunei, Burkina Faso, Burma, Burundi, Cambodia, Cameroon, Cape Verde, the Central African Republic, Chad, Mainland China, Comoros, Congo (Kinshasa), Congo (Brazzaville), Cuba, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Guinea, Guinea-Bissau, Indonesia, Iran, Ivory Coast, Kazakhstan, Kosovo, Kuwait, Laos, Lebanon, Libya, Macedonia, Madagascar, Maldives, Mali, Marshall Islands, Mauritania, Micronesia, Moldova, Mongolia, Montenegro, Morocco, Mozambique, Namibia, Nepal, Niger, North Korea, Oman, Qatar, Russia, Rwanda, Samoa, São Tomé and Príncipe, Saudi Arabia, Senegal, Serbia, Somalia, Sudan, Syria, Togo, Tunisia, Uganda, Ukraine, United Arab Emirates, Uzbekistan, Vanuatu, Vatican, Vietnam, and Yemen. So there are definitely options.

The Word on Meetings

Dear *2600:*

How do I set up a *2600* meeting in my town?

Marthalamew

We get asked this question so often even though we have all of the info up on our site and in every issue. But we all have to understand that there is a constant influx of new people who are hearing this for the first time. (This is also why material many of us are already familiar with gets repeated occasionally in articles.)

To address the question, it's relatively easy to set up a meeting. First, make sure there isn't one already in your area or nearby. Then, find a nice public gathering place. Food courts and coffeeshops work best. Ideally, you want a place where literally anyone can stumble upon your group and join in the conversation. That, after all, is the whole point. At first, you may well be the only one there. This is where most people give up and walk away. If, however, you stick around and do whatever you can to get the word out (flyers on bulletin boards, notes stuck inside copies of our magazine in local bookstores, full color highway billboards if you have the budget), you'll find in most cases that there are indeed more people out there who will show up. Lastly, you need to keep us informed. We only list meetings that we know are actually in existence and, if we don't hear back from you, we'll have to assume that yours isn't. Then your meeting won't be listed in the magazine or on the website (www.2600.com/meetings) and far fewer people will know about it.

So, in short, you need to do the research, show some initiative, be patient and keep trying, and communicate. These, after all, are attributes a good hacker should have in abundance, and it's why we continue to have so many successful meetings worldwide.

Dear *2600:*

Taking on board your response to my previous letter (it did seem stupid when I saw it written down), I have decided to restart the Glasgow meetings. I have also created a shiny new site for the meetings: 2600Glasgow.com.

TheGeek

That's the spirit. We look forward to more updates.

Dear *2600:*

I went to Tenders tonight in Huntsville, Alabama and there wasn't a meeting and the staff had no clue what I was talking about. Went to Makers Local 256, and the guys there said that they met last year, and that was about it. Most of the people now hang out at the maker space. Just a heads up, so others don't try to go to the meeting when there isn't one. Great magazine though!

Tom

That's truly a shame. Having spaces to hang out and work on projects is great, but nothing can replace being out amongst the public where you constantly find new people to interact with or even recruit. That's how communities grow. We hope to see this meeting come back to life someday.

Dear *2600:*

So, hi I'm living in Turkey and I wanna meet you over here.

Magacimaga

It's possible you might not know what meetings are all about, so please go check out our website before we have a colossal misunderstanding.

Dear *2600:*

The Beit Shemesh, Israel meetings are still fairly small but stable. Ironically, nobody bothers calling the 1800 number. Not even the Safed meeting. Expected a flood of calls.... The *2600* sign and displayed magazines do attract curious questions, which is always fun.

Faqanda

We're also dismayed at the number of people who don't use phones for actual talking these days, but, as you are seeing, there is still a spirit of curiosity out there, both within and outside of the hacker community. It's those interactions which make it all worthwhile.

Dear *2600:*

Greetings. I live in Gothenburg in Sweden and I was wondering since I looked at your list and saw that the meeting was going to take place in Stockholm, maybe you guys could change it from Stockholm to Gothenburg?

Flipchan

Let's see if we understand. You want us to move an existing meeting to your town simply because that's where you live? It's possible that this may be inconvenient to those people who aren't from your town, which is why we're going to discourage this. However, there is nothing stopping you from starting a meeting in Gothenburg, as it's literally on the other side of the country and probably a great place for hackers to get together.

Dear *2600:*

Alas, it was only myself and one other body I had dragged along that made this meeting this month. I have, however, created an email address and linked to it from the site, so hopefully as we carry on, more will join.

TheGeek

It's almost guaranteed that this will happen once word truly gets out. It's easy to become discouraged, but if this wasn't a challenge, everyone would be doing it.

Dear *2600:*

I came across your site on a Lainchan post and have a few questions: Do I need to sign up somewhere before I go? I'm in The Netherlands, so I'm going for the Utrecht meeting.

Anything specific I should bring with me? I have a Toughbook 19 MK5 tablet/laptop, a Toughbook U1 UMPC, and a Nokia N900. Is there a specific theme to the meetings?

Dennis

Please just come as you are and don't worry about what kind of equipment you have or your level of expertise. Our meetings are traditionally quite different from anything else you might expect. First off, they're not actual "meetings" in that there is no one person leading a discussion. It's simply a gathering of people who share a general interest in the hacker world. There is no initiation or minimal level of knowledge on any topic. You may know something about phones but nothing about computers. This is perfectly acceptable. Nobody should feel excluded unless they are actively working against the spirit of the hacker community, which is to explore, answer questions, share information, and experiment on all levels. Obviously, we can't guarantee that you'll find something in common with others who attend. But making that effort is what's gotten us this far.

Dear *2600:*

Hello, we are a bunch of college students who are interested in InfoSec and would like to hold meetings in our town, first Friday of the month at 1800 in Starbucks on 246 Broadway Street, Chico, California. Please post in your magazine, thank you.

Ex Tenebris Lux
Semper Technocracy

We don't usually do it this way, but we'll alert the world through our letters column as well as in our meeting section. It's up to you now to keep us updated on how the meetings are going. Good luck.

Dear *2600:*

Any word on whether the Pittsburgh meeting still exists or not? I saw it in the last issue, so figured I'd venture out and it doesn't seem like anything is going on. Wanted nerd time. #sadface

Philip

You wrote this to us less than ten minutes after the published start time of this meeting, which is way too early to conclude that nothing was happening. Often, people show up an hour or two after this. We suggest people who are the first to arrive simply hang out and use their laptop, read a book, or (best of all) have a copy of 2600 sitting in front of you. If you do this for the entire length of the meeting and nobody else shows up, then let us know. In the meantime, try to stay positive.

Dear *2600:*

I am a former attendee of *2600* meetings in Sydney, Australia. I moved to Colombia in November of last year and have been missing my monthly *2600* activities, hence the email to begin the process of getting a *2600* meeting underway here in Medellin, and potentially in Bogota, the nation's capital.

I'm planning the first meeting and have taken the initiative to ensure there are participants to show up before committing fully to the cause. Let me know if you guys need any more info. I am keen on getting the website up and running to advertise and also confirm location. At this stage, it's looking likely to be held onsite at the University of Antioquia. There's a cool university bar there that could certainly cater to needs.

Richard

This is a great idea and we're happy to see you planting the hacker seed in another part of the world. We hope to see this one really sprout.

Dear *2600:*

There is a new meeting starting in Tacoma, Washington this coming Friday. It will be held at the Tacoma Mall in the food court at 6 pm. We will notify you after the meeting to let you know how many attendees we had.

Rebecca

And this is all we ask. We wish you luck and hope it all goes well.

Dear *2600:*

I wanted to request more information about the *2600 Magazine* meetings. I would like to know what the meetings cover, as well as what the cost is to attend a meeting.

Sean

If we were evil, we could get away with so much. But no, there isn't a charge to attend the meetings that you pay us monthly as long as you don't tell anyone else. They are free and open to everyone. There is no agenda, other than an interest in hackers, the magazine, and being somewhat social for a night. Go and have fun.

Dear *2600:*

We hosted our first meeting in Tacoma, Washington yesterday. We had three people come out. We had a talk about kidnapping and rescue from a security specialist and what we would cover in upcoming meetings.

Rebecca

Well, that's an unusual topic for a meeting, but being unusual is actually quite typical for one of our meetings. Thanks for updating us and we hope future meetings go smoothly. Presentations aren't necessary unless you really want to include them. Most important is that nobody feels excluded for not being interested in one particular subject. There should be lots of areas for attendees to retreat to and talk to the people of their choice.

The Fight for Justice

Dear *2600:*

I am taking out a lifetime subscription because I hope the injection of funds goes some way to help you guys stay alive after the rip-off by the nasty corporate distributor scammers. Great mag!

John

We really do appreciate such generosity as we're still trying to recover from this. While it would take nearly 400 people doing the same thing to get back the money that Source Interlink (now known as The Enthusiast Network) didn't pay us for issues they sold, being able to shame them publicly for their business practices makes it a bit less painful. (We'd be most grateful if our readers helped to maintain their Wikipedia pages so their actions remain a part of their history.)

Dear *2600:*

For the first time ever, I had to put down your magazine in anger. Not at you, but at the letter in Winter 2014-15 of the autistic in prison (I can't reference his name; I'm in the hole right now). As an autistic person in prison myself, I know I'm fortunate to be 6'2" and 230 pounds. Even still, there isn't any way to explain how overwhelming these types of places are for an autistic person. I've been in for four years but designated five times already, been in multiple "fights" (usually me vs. multiple gang members... you know, a fair fight). Had my head cracked open and stapled shut, nose broken, eyes swelled shut, had a tooth go all the way through my lip once. Meanwhile, every time, it's me that gets transferred because *I'm* the liability. When my head was split open in the one fight, the incident report claimed I had a "scrape" on my head. A scrape. Really. Meanwhile, after another "fight," they threw me in the hole (for my protection) and terminated my visits (for my protection). My case manager would ignore me. He'd walk through, talk to everyone else, but walked past my cell saying "I'm busy!" Meanwhile, without a word, transferred again.

While I know this is not much compared to what the other autistic guy went through, I know that the general treatment of autistics in prison is absolutely piss-poor. I've seen so many similar stories to his in *Prison Legal News* that make me set down the magazine in rage as well, and I wish I was surprised to read it. Instead, I'm just angry. I know there's nothing I could say to him to make his situation any better. How they can claim that this kind of thing isn't "cruel and unusual punishment" is a sick joke. People claim that autistic people lack empathy? I'd say our government has a hell of a lot less empathy than *any* autistic person I've met. And I'm so tired of the bullshit "budget cuts" excuse. I bet if the rapist gave HIV to a prison guard, they'd find the money. Ridiculous.

P.S. Another request for bound *2600* digests as well, please.

token

Dear *2600:*

Today is a bad day in Germany because two online journalists are being officially investigated because they printed and commented on leaked documents. This is especially ridiculous because the same government agency did nothing against NSA and Company tapping our phones for years including those of our prime minister.

HJT LED-Professionals

You're referring to two journalists from the publication Netzpolitik *who were put under investigation for treason after publishing some information which rubbed some German authorities the wrong way. From leaked documents, they revealed details about the expansion of a surveillance program targeting the Internet that was being run by the German secret service. If nothing else ever demonstrated the threat that journalists face on a daily basis when reporting the news, then this does in very clear terms. The fact that authorities cannot differentiate between the source of a leak and the reporting of a leak is extremely troubling. How much faith can any of us have that these authorities will ever investigate or question the le-*

gality of what the leaks themselves uncovered - or do anything short of trying to lock away anyone who dares reveal such useful information, which the public has every right to know? This is why organizations like WikiLeaks are in true danger. It's why people like Chelsea Manning are in prison for revealing outrageous injustices and it's why Edward Snowden finds it impossible to come back to the United States.

This particular story from Germany has a (so far) more positive outcome, as the investigation was stopped after a massive public outcry. In fact, the prosecutor who started the investigation was fired, which certainly made many in the free world feel a little better. But these things never really end and we're certain there will be more threats to contend with in the not-too-distant future. We appreciate our readers keeping us all in the loop.

Dear *2600:*

Hey *2600* community, it's Ghost Exodus. Here's a case update, as I need awareness.

A few months back, my legal team coordinator (LTC) found out that a fat chunk of recorded jail phone calls were deleted from my electronic case file CDs - evidence I could have used to exonerate myself of witness intimidation against the cooperating witness who informed on me six years ago. The only "evidence" against me was my prosecutor's own oral testimony. After accusing my lawyer of using his e-mail to conspire against her, he created a new e-mail, which he replaced on his letterheads. She tried to put a restraining order against myself and LTC, accusing us of hacking and criminal association with Anonymous in a motion to my judge. We could really use help with putting a FOIA together to obtain the BOP's copy of the removed phone recordings. You can kill the protester, but you can't kill the protest.

Jesse McGraw

Dear *2600*:

I was sorry to hear that you got ripped off by your distributor (again). Maybe what needs to happen is for the small publishers to set up a co-op distributor or something. Maybe the print-on-demand model would be better for *2600* and similar magazines. Worst case, I bet you could use Kickstarter to stay afloat. Good luck!

Dave

Thanks for the ideas and good thoughts, but we intend to try and ride out the storm by continuing to put out something that our readers want to buy. We're open to all sorts of alternative distribution plans. The important thing is that we not let something like this defeat us.

On Payphones

Dear *2600:*

I am an old telephony guy (who actually worked on payphones back when Super Glue first came out... what a mess... at times it was like winning at slots when you opened them up) who got dragged into the datacom world around the time 10BaseT was starting out and I do remember your mag from *wayyyyy* back then. Glad to find you still at it.

I am living in the Cocos (Keeling) Islands now and there is actually a working payphone here! Nothing special, but it is here. Would it be worth a subscription to send a photo? I so would like a subscription again. I can't imagine you have a photo from this part of the Indian Ocean with a working payphone, but then again, who knows, it may have been done. Let me know. If you search Cocos you may find some interesting stuff.

Gerald

It's absolutely worthwhile to send us your payphone pictures from wherever you happen to be. Even if it's a part of the world we're quite familiar with, your photo may be particularly unique and historic. But please try and resist the temptation to rip this payphone open. That was never part of what we stood for.

Dear *2600:*

There was an interesting article in the *Detroit Free Press* titled "Last Call for Some Detroit Pay Phones" (July 25, 2015).

Scott

Thanks for forwarding that. It was indeed interesting to read about the steady decline of the American payphone, particularly in states like Michigan where the payphone to human ratio stands at 20 per 100,000. (Hawaii leads the list with 296 per 100,000.) Back in 1984, a busy street corner payphone could net $200 a week in coins and today it barely brings in $5 over the course of a couple of months. So yeah, you could say there's a trend of sorts in the payphone world. But one thing which we found pretty amazing was the amount of photos they decided to print of payphones and their remnants, each one with a little explanation below it. Where have we seen that before?

Queries

Dear *2600:*

I thought I remember seeing a line in the magazine that said I could chose to get paid money or have a year's subscription. That may have been a few issues back. Did you ever offer money for articles or still do upon request?

sm

The only piece we're able to do that with is the Hacker Perspective column, for which we pay $500 when printed. We get lots of submissions for that, so we can only accept new ones occasionally (we let people know this inside each issue). For other articles and photos, we offer t-shirts, back issues, or subscriptions. And letters like this one simply carry the pride and immortality of having appeared in our infamous letters column.

Dear *2600:*

Could you tell me where I can buy a copy of the magazine near me? My zip code is 60553.

Bill

We're sorry to say we have no easy way of doing this at the moment. We can tell you that we're carried in a Barnes and Noble in Rockford, Illinois, which is around 30 miles from your location. But something as simple as a searchable database where our magazine is sold is something we can't seem to get our hands on from our various distributors. Some will give us the info and others will keep it to themselves, thinking a competitor will use it to their advantage. In the end, less people know where to find us, which hurts everyone.

Dear *2600:*

I've been reading your magazine for two decades now and I wanted a *2600* shirt soon after I picked up my first issue. The problem is I'm seven feet tall and slim. Standard sized t-shirts never fit properly. If they're long enough, they're always roughly the same width as a tent.

My question is this (and I know this is absolutely a shot in the dark): If I'm able to source tall-sized black t-shirts and have them delivered to your offices, would it be possible to have them printed with your next run of shirts? The designs I'm interested in are the new traditional blue box and the government seal. I'd pay your regular shirt price for this service.

Again, I know this really isn't likely, but I had to ask. Regardless, I'll always be a fan of your publication and I urge you to keep up the good work. We need more voices like *2600's* in this world.

Daniel L.

We can certainly try to make this happen. We are inquiring with our printer to see if this can be done. We don't see any reason why it couldn't be, but we suspect we would have to wait for the next printing of blue box t-shirts. Our government seal t-shirts, however, are no longer being made (unless you're referring to the government seal sweatshirts, which we're still producing). Our office staff will follow up with you on this.

Dear *2600:*

While searching for a pen name I used for an article, Google found this: http://2600.wrepp.com/2600/OpenSource/Data/Authors.txt. What is it? Seems like it shouldn't be publicly accessible nor indexable.

Anyways, you guys have an awesome culture regarding incarcerated hackers. Thank you for everything you have done and are doing. If I can be of voluntary assistance to *2600*, please reach out.

nychacker

Thanks for the offer. As for the URL you found, this was an author index project started by one of our readers and it consists of information contained within the magazine, so there's no concern with it being publicly accessible. We imagine it's proved quite useful for readers and writers alike.

Dear *2600:*

I want 2 be a hecker... Help mr

Bhaskar Das

Wow. Well, you did write to us, so the word "hacker" is probably what you meant. Although "hecker" is one letter away from "heckler," which some would argue is something you could certainly be considered. But if it's "hacker" you meant, you're probably going to be hearing from a bunch of them pretty soon, so you can ask all the questions you want. We often wonder just what it is people expect us to tell them when they ask us questions like this, questions we get so frequently that it's both funny and depressing. Maybe all we have to do is anoint them as official hackers (for a sizable fee) and they would be content. It's worth considering.

Dear *2600:*

I was wondering why *Off The Hook* didn't appear in my incoming podcasts, and it turns out that your SSL certificate has expired: "www.2600.com uses an invalid security certificate. The certificate expired on 06/08/15 01:59. The current time is 07/08/15 17:20. (Error code: sec_error_expired_certificate)"

Adam

Yeah, about that. We believe in SSL certs, we really do. We've been pushing for encrypted content as a default on the net for decades. What we don't believe in are companies that take advantage of this and make a small fortune out of fear and pressure. The amount of money being spent to basically have a "trusted" company say that you are in fact who you say you are can amount to hundreds or thousands of dollars a year per site - even per sub-domain if you're not careful. Of course, we became "untrusted" as soon as we didn't pay up. And this after we became "trusted" when we provided fake info in the first place!

We know we're getting a bit of criticism for not playing along and using these services. But no type of personal communications on our site is involved here (like emails, passwords, or any sort of customer data, etc.). All of that takes place on different sites that always are encrypted. Here, we're discussing people who just browse our regular website, download radio shows, etc. But that information should also be encrypted, as there are some countries and households where scrutiny of what you actually did on such a site could come back to haunt you. That is why we're opting for the new "Let's Encrypt" option of SSL certification that's rolling out later this year, is simple to use, and free. More details appear in this issue's EFF column.

Dear *2600:*

Hi,

Firstly, I'd just like to say great job on the success of your site 2600.com. You have a great collection of some really interesting articles! I really like your payphones around the world feature too.

The reason I am writing is to let you know about Ezoic. Ezoic is the first Google AdSense certified partner blah blah blah blah blah.

This email was sent individually to you. I personally visited your website and thought it would be a great fit for our website testing platform. You

are not part of an email list, however, if you would prefer to not receive any more emails like this one from me, please visit http://www.ezoic.com/email_preferences.php Ezoic Inc. 2542 Gateway Road, Carlsbad, CA 92009

Piper

Nice try there with the personal touch. We almost believed this was an actual reader when they alluded to our payphone feature. Spam is getting more sophisticated every day, but we intend to keep well ahead of it. We do wonder how on earth we're not on an "email list" if you intend to send us more emails. And by the way, we visited 2542 Gateway Road as you suggested above to let you know personally our feelings on the matter, but nobody was around. True, it was 4 am, but still. The net never sleeps.

Dear *2600:*

Back in 2005, I was charged with computer crimes without any proof that I actually committed said crimes. The forensic computer tech used data recovery software called EnCase, which you are probably familiar with. In 2009, I was charged again with computer crimes. The same computer tech was given the task of going through the same hard drive from 2005. He stated that due to new and updated technology, he would possibly be able to recover more evidence than before. The tech did find more evidence, but again no evidence that I committed said crimes. The tech used EnCase again in his second time going through the hard drive. So my question is has EnCase had any advancement or updates in its recovery process between 2005 and 2010? If you could give me some insight, that would be very helpful.

Steven

We don't doubt that there are advances made in this field and with this particular product every year, and certainly there would be significant improvements over the course of five years if they expected to stay in business. If the case against you is circumstantial, then that is the angle to attack rather than the software they're using. All it can do is tell you what's there. It can't tell you the why or the who.

Dear *2600:*

Since 2001, I've had a TracFone, and I haven't had any more problems than the minutes not coming through sometimes. I check it occasionally to be sure most functions I need function, such as speed dial. Yes, I did say TracFone. What I didn't say was it's a Motorola V170. Aye, 'tis ancient. I got it originally for emergency use at religious festivals. Up until a few days ago, no real problems. I left in the morning the other day and, before I got out of the complex, I saw a neighbor's dog running loose, so I tried to call him as he is also a healer. I had him on speed dial. Imagine my surprise when I got a fax machine, knowing he doesn't have one in his home. So then I brought the number view function up and, lo and behold, where I had his home number was something totally different.

I did not think about it then, presuming I goofed. When I returned home, I pulled the phone and started checking numbers. *Wow!* All but a few numbers were altered from the original correct numbers. My first thought was that TracFone was having a problem, so I called them to no avail. They "...had never had such a thing happen." Then I checked the charger voltage every few hours for the next day. No problem. While I normally leave it on except when shopping, it's not a smart phone, so if any of you true techies out there know how this venerable device could have been cracked, I'd like to know. Thanks all.

Captain Cautious

Kindle Karma

Dear *2600:*

I'm sending you the strange date issue we are seeing in the Kindle version. I'm not sure what sort of meta tag or data they are pulling this date from, but I see this on my Android phone and iPad versions of the Kindle app when reading *2600*. I think it's only shown up on the most recent two or three issues, so they might have changed the Kindle app to read some extra data that you're not populating somewhere in the published file you are giving them.

Josh

This was a ton of fun to try and figure out and the Kindle people said the problem was on their end. Even after that, it took a whole lot of time for them to figure out the fix. But we're told it's no longer happening. Please let us know if you see anything else amiss.

Dear *2600:*

Did you know you can get your *2600 subscription* sent to non-Kindle devices? It's not automatic like the delivery to Kindle, but it's an answer to some of the problems we digital subscribers have (like previous issues being replaced by the current if you haven't specifically saved it). I know you've started putting issues out as individual digital books, but this will help people already subscribing. Please get the word out!

Instructions:

Go to

Your Account > Manage Your Content And Devices

Show > Magazines

Actions > ...

Deliver past issue to my...

There's also a download and transfer past issue via USB, but I think that's in DRM hell.

Steve T. in Manhattan

Dear *2600:*

I'm glad to see that you managed to get the header fixed on the Kindle edition. It now shows the proper date. But as of this issue, I can no longer see the cover graphic, nor can I navigate to it from the article list. Always something....

Of course, I can survive without the graphic, but I know I'm not the only one who spends time

poring over the cover for its artistic and creative merit. I hope that can eventually also get fixed.

Kindle woes aside, keep up the good work!

Saskman

We're really sorry this happened and we don't have any idea what caused it. Suffice to say, if you're a Kindle subscriber, you received a replacement issue once we alerted the Kindle folks of this mishap.

Weird Mail

Dear *2600:*

"Rae, Christine, & Richard" have been stalking me at home, for 3.2 hrs, threats & $s extortion.

A Suscriber

And we're the ones you decide to contact with this info? Good God. First of all, we don't monitor incoming letters every day so by the time we saw this, your saga had undoubtedly progressed into whatever the next stage of this would have been. Second, what on earth are we supposed to do with letters like this? Sprinkle magic hacker dust your way? Call the authorities? Turn on the news? We really don't know what people think we're capable of and it's probably best that it stay that way. Finally, and to completely trivialize whatever was happening here, we don't know anyone who's not a machine who measures time in this way. 3.2 hours is three hours and 12 minutes, which is also a bit too precise a phrase for humans. It just seems like a weird time to get all digital.

Dear *2600:*

I need help finding my black hat hacker. I believe that my brother who has psychopathy has hired a black hat hacker to freaking mess with my life. It has been difficult to deal with this and I want this to stop. Please help. My smartphone is not always working now thanks to this or my house phone. But the number is [redacted]. Home phone [also redacted]. If anyone else picks up like my roommate or my mother just ask for [super redacted]. Please just say it is a friend because I don't want my old mother to have to worry about this.

Thank you for your help.

[We Are Not Printing Your Name]

This is a direct result of how the media portrays hackers. Thanks, guys. Now every time somebody has a bad day, loses their keys, has the cat puke on the good carpet, it will be because of something a "black hat" hacker has done to them. And the only way to fight this fire is with more fire. This hysteria helps to sell all kinds of products and put people in the limelight, but it's incredibly destructive, not only to the hacker community but to the general populace.

Sure, it's possible to be messed with through your phone or computer - even your television or doorbell can join in the fun these days. Cars, planes, baby monitors... everything can be hacked in some form. But the number of people we hear from who believe some crazy Hollywood script is playing out inside their living room is simply astounding.

To those of you who are convinced that something is indeed happening to you involving technology, please give us the specific details. Maybe we can help figure out what's actually happening. To the rest, please take with a huge pillar of salt any reports of the evil things that hackers are up to, along with meaningless designations like "black hat" and "white hat." Hackers are experimenting and revealing all kinds of interesting things, but they're not the villains from a James Bond film. You'll just have to trust us on this....

Dear *2600:*

Congratulations to Source Interlink for successfully "hacking" your naivite, and "Occupying" your revenue.

You Blue-Pill SocialJusticeWarriors fucked yourself... again. You never learn, do you?

Red-Pill Guy

And again we have affirmation that we make all the right enemies.

New Stuff

Dear *2600:*

Your readers might like an entertaining article on the disassembly of an old boot-sector virus. They are obsolete now, but the code is fun to read about. The article would have lots of 8086 assembly listing in it. Here is the existing work: http://www.computerarcheology.com/wiki/wiki/Virus/Stoned

Thanks for your time and consideration!

Chris

This is precisely why we encourage people to send us articles and not simply post them online. For one thing, that disqualifies your article from being printed, as we promise our readers new and unpublished material. Second, as anyone going to that link has already discovered, what's online often doesn't stay online, at least not in the same place. Once you print something here, it's forever. The printed word cannot go away and it can't be revised, which is what makes writing an article here such a true piece of history. We hope to see more people send us material before publishing online (which you are free to do after we publish it here) so that your work is truly appreciated and remembered.

Dear *2600:*

I have been toying with an article for some time. The idea initially occurred to me after the fallout from the Edward Snowden affair. I have sought an unbiased publisher, but the government rags (in which its publication might actually do some good for Uncle Sam) are too wedded to incompetent vendors.

The article has do with why our information security capabilities are in the state that they're in and what could have been done about it - if our government cared one whit. Developments make it crystal clear that they have already surrendered

their technological and military superiority to China and, moreover, are expending ever less effort on even putting on a "show" to caring about computer security. Meanwhile, each "expert" we see is more readily buffaloed than the previous buffoon: an RSA "consultant" was on Fox News the other day who (a) didn't know what RSA stands for and (b) explained a recent hack as - get this - the attackers "went into" the system. "Went into."

Here's an attached resume to indicate that I'm not some abject moron. Something tells me you will find it as unique as I know my written perspective is. Trust me, I'm nothing like the others, and I long since tired of lifting a finger to help our government.

From a technical perspective, I won't go into the details of ad hoc hacking techniques as it were, but I have plenty to share on the underpinnings of high-assurance military systems, which - I guarantee - are way beyond the lion's share of your readers, both from the historical exposure perspective and the formal mathematics perspective. Don't be so quick to dismiss everything that comes from DoD because Joe Schmuck leaves a guest account undeleted.

B

We would never dismiss any source of information and we have over the years gotten much valuable material from within various institutions that others might find quite surprising. Please do write your article from your unique perspective. There's no need for resumes (impressive though yours is) or any sort of other "proof" of your abilities - we think your words will speak for themselves.

Dear *2600:*

Let me say at the outset that I am not a hacker and, until last year, I knew very little about the subject. I'm an established author who writes thrillers for a living and was formerly a television news executive.

Then, early in 2013, I came across a newspaper report about a woman whose webcam had been hacked. The man responsible had spied on her for some weeks and had managed to record her in compromising positions in her bedroom.

This aroused my interest and, over the following couple of months, I researched the subject thoroughly. I trawled the Internet and checked out all of the hacking sites including *2600*.

I was both amazed and appalled at what I discovered. I had no idea that webcam hacking was so widespread or that more and more of the hackers were resorting to blackmailing their victims. I came across the term "sexploitation" and read about so-called "ratters" and how they collect "slaves" and sell access to their computers.

For a writer of fiction, this was all very fascinating and it prompted me to start developing a storyline. It took me several months to come up with a plot and a cast of characters.

The result is a novel called *Malicious,* which was published in November 2013 by Global House Publishing. Amazon Worldwide has exclusive rights to the ebook and paperback for a limited period.

The book focuses on a female detective based in Houston, Texas who becomes a victim of a hacker calling himself the Slave Master. The detective is perfect prey because she is addicted to online porn and has therefore exposed herself on many occasions in front of her webcam.

My story is pure fiction, but I know from what I've read that this sort of thing is going on across the world at an alarming scale. Mature women and young girls are falling victim because they're not aware of the problem.

I myself now make a habit of covering up my webcam and I'm sure that those who read my book will be doing the same in future.

Malicious is my eighth thriller and, for anyone who is interested, it's available on Amazon. There's more information on my website, including a video trailer, at: www.james-raven.com.

James Raven

Congrats on the book, but we're dismayed to see hackers once more being portrayed as the villains based on your description above. Just because someone is able to exploit a vulnerability, they do not automatically become a hacker. You'll find that hackers spend endless hours figuring things out, designing better systems, and sharing their results. Whether someone else decides to install a system a hacker has designed or make use of a vulnerability a hacker has uncovered, those people have their own roles (good or bad) in society. Making use of hacker knowledge does not a hacker make.

Advice Needed

Dear *2600:*

Hi *2600!* Please publicize this if you wish.

I adore your achievements, your goals, and your motives. I am far from a hacker of any kind, but find *2600* great, like an "information revolution."

No doubt I've developed problems with big, overgrown powers that attempt to control us. To really assert ourselves has become a civil fault or a crime.

This question requires a specialized IT person like a hacker to answer with a fair opinion. Being a legal issue, I refuse to pay a lawyer to decipher what should be freedom of speech, plain and simple. I'm not requesting legal advice (but any insight is useful). Much better may be in general what you people with sharp experience here think may happen. I'll summarize this legal puke in bullet points:

1) I hired and paid a lawyer who purposefully did not communicate with opposing council, a fair offer to end this case.

2) Because I caught him, I instructed him to do as he was hired to do, in apprehensive, strong text.

3) He used that to withdraw; he did so *after* I paid in full.

4) The judge allowed this regardless of my objections. The state's bar was no help at all - I had to hire another lawyer.

5) My only recourse would be to sue him in court. That's his game aside from his running for; you guessed it, public offices.

6) Since (in my field) I've directed over 100 sizable website builds, I know SEO well, IT in general, and especially, "reputation tactics," i.e., how to leverage negative (or positive) links to appear with, under, or before one's domain upon a search for that entity. That's in my playing field.

7) Before ruining his online reputation as an attorney, I provided fair warnings: to refund me in full or it'll cost him much more in lost revenue. My threats were simple, honest, and logical - not with angry or vindictive grammar. I'd state only facts, truth, all verifiable as to what he did, fully documented, and then why according to my opinion. I'd then promote this to our public, essentially local. Do we all not have that right? Naturally, he did nothing within the time I gave him. Therefore, I created a WordPress "review" site under "his" name, other static domains with reviews on "him," then posted my factual story into several review venues such as Yelp, Google Plus, Facebook, YouTube, general replies under his posted articles, etc. These now come up upon a search for his name directly under his own links. It must've worked well.

8) He with our state recently subpoenaed WordPress under criminal investigation for all contact information of those sites. The subpoena read, "The State of [redacted] vs John Doe" for demanding this information.

9) That request seems illogical since I'd stated my name several times within all text, along with my contact info as the author. I even wrote why this was done, that (at first, under my owned domains) all can be removed with my offer to cease upon refunding me. My threat continued in that most "other" review sites not under my control are very hard (or expensive) in deleting complaints. By that point, I demanded damages since he'd hurt me (and my family) much more than his fees can warrant.

10) In addition, the subpoena stated clearly: "This request for information is confidential. DO NOT NOTIFY SUBSCRIBER/DO NOT CLOSE ACCOUNT." I found this most interesting. If I'm not reading that wrong, then WordPress emailed me their subpoena against the state's demand. Is the WordPress admin telling me something, like to take these sites down?

The questions are: What acts were done that were criminal? Do we not have freedom of speech? Why are there review sites? Even if a review is incorrect, how can that be considered criminal? Why was this contact info demanded when I stated that I wrote this providing contact info?

Thanks again entirely.

JEDLUP

All of this is because of the action you're taking against the lawyer who you hired to represent you in another case? Honestly, this is more legal action than we're comfortable with.

That said, we're not sure what an IT person would be able to help you with here specifically. It sounds like you had a decent plan to attack this guy's integrity and you implemented it effectively enough to really piss him off. Legally, as long as you didn't misrepresent yourself as him, there's not a whole lot he can do against you, other than try and act like there is. It sounds as if he knows full well it's you and realizes he can't stop you legally, so is instead trying to intimidate WordPress into just taking down the content. This kind of thing has a history of backfiring rather badly for the intimidator. As to why WordPress forwarded you the demand not to notify you, it could be because there is no legal standing to make such a request or (the reason you should never discount) it's because someone screwed up.

You may need to deal with the loss of whatever you paid this guy if the courts predictably favor him as an insider - and learn the valuable lesson of never paying anyone in full until the job is completed satisfactorily. But be comforted in the knowledge that your words are doing more damage than anything else, words that he knows are coming from you. Losing money sucks, but your words having a true effect on a desired target is priceless. Trust us - this is one thing we know well. We hope it all works out.

Dear *2600:*

We are a Mennonite company who employs Amish. We were hacked two times (including our payroll). Who do we ask to teach us to break into this temporary e-mail so we can learn to protect ourselves? Thank you.

jennifer

We're not sure what being Amish has to do with anything, as computers are used, albeit somewhat sparingly, in this community. Common sense procedures are the same regardless of experience. Using secure passwords, not opening attachments in email without knowing the source, avoiding trusting unknown outside entities with your private data... these are the basics that apply to everyone. Now, concerning this breaking into some temporary e-mail to protect yourselves - we're not really sure what that's all about. If you think hackers can just break into something and fix your problems, that's a mass media myth. If you have data being held hostage in some account somewhere, there are possible steps you can take to retrieve it. None of what you're trying to do is very difficult or beyond the reach of anyone who chooses not to blindly buy into all of the technology we're surrounded with. We hope this helps.

Digital Editions

Dear *2600:*

I'm wondering if lifetime subscribers can also obtain copies of the magazine in formats beyond the paper copy at a discount.

What I'd be interested in is an electronic copy of issues as I can afford them (past, present, and future). The ability to search will be great! Yet at the same time, I enjoy the paper version, especially right now - as I just got the word I have cataracts in both eyes.

Bertram

We're sorry to hear that and be assured that we're considering all possibilities with regards to digital editions. It's a tremendous amount of work to organize and put out properly and we have a long way to go. To do something in conjunction with existing lifetime subscribers requires integration of databases and it doesn't do anything for those who subscribe by the year or who buy issues at a bookstore or newsstand. Until we come up with the perfect solution, we're trying to make the digital editions and digests as cheap as possible.

Dear *2600:*

Have you considered bundling the digital with the hard copy edition of *2600?* Also, I have a couple of periodicals that give away the digital to subscribers.

And for those of us with decades-long subscriptions, might you offer free access to any issue that was published during which we had a hard copy subscription?

Why would I want the digital? Because having the collection would allow me to avoid digging through mountains of paper products and tech.

Just a thought.

Eric

These other publications most likely have advertising and other means of support to allow this. Our digital efforts have basically doubled our workload over the past few years as we continue to digitize our entire back issue library. As we don't keep our subscriber info online for security purposes, we'd have to develop a different process to tie that into something like access to digital copies. We're not saying this can't happen, but our hands are really full now and we're trying to just get the job done. We believe there are currently enough options so everybody can get the versions they want for very reasonable prices. But we are always trying to improve.

Dear *2600:*

I am a lifetime subscriber to your magazine. I would like to know if I could switch to the digital subscription.

Ruddy

This option isn't possible for the simple reason that we don't have access to digital subscriptions that go through Kindle, Nook, Zinio, or Google. Those are transactions between you and those companies and you're as anonymous to us as you would be if you bought a copy in a store. Also, none of those outlets offer lifetime subscriptions anyway. As we continue to expand, we may be able to put something together in the future that can handle this.

Turning Point

Dear *2600:*

I suppose it's hacking, although I've always considered it curiosity. From as early as I remember, I'd no sooner get bored of a new toy than have it taken apart to find out how it worked.... Sometime in the late 70s - early 80s, there was a radio controlled car - a Christmas present I think - that my younger brother had tired of. I knew that CBs and scanners needed frequency crystals. I also had some general electronics experience. So, tiring of homework, I opened up the little transmitter and, lo and behold, a crystal. I proceeded to unsolder it and searched my parts drawer for a viable replacement item. A variable cap tuner from a pocket radio would do fine, I figured.. I soldered wires from the tuner to the empty holes on the transmitter board and connected the battery. I turned on the transmitter, but the car was not affected in any way. How about the radio, I thought. So I turned on an AM radio and twisted the transmitter's dial but nothing, except a small scratch near the lower end of the band.

Suddenly a loud pounding from downstairs startled me. My name was then yelled followed by a stern "What are you doing up there?" Opening the door, I replied, "Just finishing my homework, why, what's the matter?" "Never mind, must be something wrong with the TV station, the problem's gone now." Needless to say, this was confirmation that my experiment was indeed a success and I had that rush of curiosity. What had I done?

I rounded up my creation and quickly made a case for it from a small box, adding an on/off switch. I proceeded downstairs for a bowl of ice cream. My parents were sitting in the den watching TV. Once seated in the kitchen with a bowl of ice cream, the TV in clear view but out of my parents' line of sight, I turned on my device. Nothing happened initially but, upon turning the dial, the entire picture squished into a thin bright white horizontal line with a loud howl of audio horror - quite disturbing. "That's what I was talking about, never seen anything like it," my dad commented. I cut the power to my device and replied that "I've never seen anything like that either - like you said, must be the TV station having issues." I finished my ice cream, cleaned up, and proceeded back to my homework with a raw sense of satisfaction.

For whatever reason, sports never interested me - there was so much more to learn, so many more important things - and this thought inspired the greatest test of the incredible power of my little device. It was New Year's Day and all the neighborhood was gathered next door for *the game*. I sauntered over with my little box. It's not that I wasn't invited, so if I was seen I could just say I was seeing how the game was going. I went to the back sliding door and peeked in. Everyone's eyes were fixed on the TV and all kinds of coaching comments were being spewed. No sooner did I take this in than a commercial came on, at which

point I quickly darted out of sight.

Now was the time to plan. Once the game started again, attention would be fixed and I'd have at least ten minutes until another commercial. I waited until I heard everyone yelling and coaching again and returned to my observation window. I waited for the perfect moment: a pass. It wasn't long and there it was: a lot of open field and a long pass. At this moment, I flicked the switch and the game condensed into a bright white line. The only difference was that the TV's horrific howl was drowned out by the screaming and pounding and cursing of eight or nine diehard football fans. I thought they might break the TV! I quickly restored order and felt oddly guilty.

Some ten years later, I came clean and admitted to my hacking. We were all able to laugh.

SideFx

We suggest 20 years before admitting to something like this. Some football fans really hold a grudge.

Dear *2600*:

I'm so glad I found your magazine. I have some things to say and ask. Here goes.

I have recently come to realize that I am a hacker (due to my very nature) after years of being told lies about hackers from the mainstream media, law enforcement, and Hollywood. I first found your magazine at a local bookstore and I was deadly afraid to buy it at first because I had no cash on me and it was during a point in my life when society was choking my soul. I was (and still am) afraid that buying *2600* and stuff from the *2600* store with a credit/debit card would get me put on some kind of blacklist. After spending the majority of my adulthood thus far finding myself as a human being, I became really interested in computers again when I took a programming class and found that I *could* do it. I started messing with hardware again and built a monster computer, learned to use Linux, etc. I'm well on my way to a great career in IT because of that. I eventually remembered *2600* and I bought it with cash for the first time just recently. You can be happy in learning that I have fallen deeply, madly, and passionately in love with *2600*. This magazine is going to be a huge part of my life and career and be a new addiction. I only have two issues I've bought off the newsstand with cash thus far, but I want to order a lot of back issues (plus Club-Mate!), which raises this question: Can I order something like a money order through the mail? I've seen on your site (which I visit through Tor) that I could use something like checks through snail mail, but part of me wants to keep as low a profile as possible. It would be awesome to have a printable form and have stuff like shipping taken into account (I have no idea how much shipping would be for stuff like a ton of shirts that I'll be wearing at home, etc.). I honestly don't see how people can order with their credit cards and leave a paper trail and not be afraid that it'll end up stored somewhere! I have bought a lot of books about hacking (like Dr. K's *Hackers' Handbook)* with cash due to this kind of paranoia. I hope you can clear up stuff like ordering through mail. From what I've seen in the back of the magazine, back issues through mail order have free shipping within the U.S.?

I'm sure you get this very often, but I'm scared to dip my feet into the hacker community. I know that not all hackers are evil (I know, because I'm a moral person). Maybe one day this paranoia will leave me, but right now I'm being as careful as I can. I'm not trying to rob people of their money or infect their computers, do illegal stuff, or be an asshole, but due to how hackers are demonized, I'm afraid that I'll be targeted in some kind of way. I'm afraid to go to *2600* meetings, access the *2600* IRC, or go to a hacker convention like HOPE for fear of my employer or the wrong person finding out and getting paranoid about me talking to other hackers and find myself getting fired or worse. I'm also afraid of being targeted by law enforcement (I read about what the Secret Service did to *2600* meetings in 1992) or that a law enforcement mole would be present and report me to my employer and get me fired or worse. I'm scared shitless to join and reach out to a community of people I know are just like me in so many ways: my brothers and sisters. It might be that the lies of the media, Hollywood, etc. are still poisoning my psyche or that my imagination is hugely overactive, but as it stands, I'm paranoid, afraid, and alone.

P.S. I think you should have a permanent message of encouragement to burgeoning newbie hackers on your website who might be as afraid as I am to order from you or read your magazine.

A Paranoid Newbie Hacker Wanting to Find a Place to Belong

It's easy to say that your fears are unfounded, but that probably wouldn't do much to allay them. There are ways to get around your concerns regarding buying stuff if you're unable to use credit/debit cards, Bitcoin, and the various other payment methods we accept. You can always call our office staff (+1 631 751 2600) and place the order over the phone. It would be shipped once we get payment using whatever method you're comfortable with. That part is easy. But the hard part is getting past these barriers that are keeping you from truly becoming a part of the hacker community. We suggest taking tentative steps at first and only talk to those people you trust. If you know the difference between right and wrong, we doubt you'll run into any problems on the legal end. As for those who insist on categorizing you because of your interests, try and get those people out of your life, whether by changing jobs or just hanging out with more open-minded types. There's no reason in the world you should deny yourself knowledge and enjoyment because of the ignorance of others. Regardless of whether or not you feel it, you're most definitely not alone.

MR. ROBOT - A RAY OF LIGHT IN A VERY DARK WORLD

by Emmanuel Goldstein

"We sign in. We tweet. We favorite. We RT. We say nothing."

There have been *so* many television series about hackers over the years and a good deal more that incorporate hacker characters or hacker subplots. Nearly every one of them gets it painfully wrong to the degree that we're left with no choice but to deplete their bank accounts and put the creators onto Interpol's most wanted list in order to ensure that they never cause such offense again. Fortunately, this is not the case with *Mr. Robot,* a ten-episode series which debuted in May. Aired on the USA Network (a cable channel I honestly forgot still existed), this program has done so well that it's been renewed for a second season. (Actually, it was renewed even before the first episode aired due to the rave reviews it was getting from online audiences. And it was supposedly put online early due to fears of - wait for it - somebody hacking the pilot and leaking it to the world before it could be promoted properly.)

Ever since *Whiz Kids* came out in 1983, I've been waiting for someone to get it right. I grew somewhat attached to that show only because there was nothing else similar at the time. But even then, the saccharin sweetness of those do-gooder hacker kids wore thin pretty quick. Plus they spent way too much time working with the cops. *Mr. Robot* doesn't present any of these problems.

Elliot Alderson is our protagonist. He lives alone at 217 East Broadway on the Lower East Side. (It's a real building and a real address, so major points right there for authenticity.) Elliot is hooked on morphine, works for a cybersecurity company called Allsafe, doesn't like to be touched, and can barely get a sentence out most times. He's absolutely perfect because of his flaws and imperfections. We don't necessarily *like* Elliot but we can certainly feel for him. He speaks directly to us off camera as his "imaginary friend" in a manner quite reminiscent of Alex from *A Clockwork Orange*, but without so much in the way of clever and psychotic humor. Elliot is the type of person you would pass on the street and never think twice about, apart from maybe wondering if he might be some sort of garden variety lunatic. No, Elliot is far from such mainstream hacker characters as David Lightman, Lucas Wolenczak, or Wesley Crusher - about as far as you could imagine. And it's about time.

Elliot's world gets more and more complex as he's pulled into a mysterious organization of the computer underground known as fsociety. The people who meet secretly in an old Coney Island building (including Mr. Robot himself) are tied into a much larger and looser network - one naturally equates its mystery and power to something on the order of Anonymous. These people come from every background imaginable, but that isn't done simply to earn points on the diversity scale. This happens to be today's reality - hacking has grown up and spread everywhere. While pasty-faced males are still Hollywood's favorite stereotype for anything tech-related, the real world is a very different place and, odd as it may seem, the world of *Mr. Robot* is a disturbingly real place.

Sure, there's a good degree of suspended disbelief that must be employed here. Hacking someone out of prison in 24 hours is a stretch (you generally need the whole weekend), as is the apparent ease with which webcams are able to be compromised and unauthorized USB drives attached to systems. The gullibility of employees working in vault-like establishments who allow their territory to be physically compromised by their worst imaginable nightmare is especially unbelievable,

but then we've all heard stories where that's exactly what happens, so that may not be so far off after all. Fixating on these exaggerations or shortcuts would be as much a waste of time as complaining about phone numbers that always follow the format of 555-01XX in fiction (which, thankfully, is *not* the case here). What balances out these little cheats in *Mr. Robot* is the fact that oftentimes it all winds up going to shit anyway and all of the efforts were for naught. And this isn't just about hacking; it's true of the interpersonal relationships that we see developing. Just when you see something formulaic approaching, the story veers off road and crashes into something else you never saw coming. It's this element above all others that makes this the *Breaking Bad* of hacking. Every week it just gets more fucked up. And more fascinating.

In each episode, New York unfurls like some kind of a foggy nightmare. Many of us have been there. Elliot's monotone narrative adds to the dreamlike state with which various plots develop. And the cinematography is akin to what I would imagine Stanley Kubrick doing with a hacker story set in the Big Apple.

There are some truly scary moments, not so much due to horror as to the revelation of what's *really* going on. It's well worth watching the series a second time knowing what you know at the end and seeing how it was all right there in front of you the whole time. It's great storytelling and the technical accuracy is an unexpected bonus. I actually saw an IRC kick/ban unfurl on a TV program exactly as it does in real life. And it totally worked as drama! (Again, as in real life.)

Full disclosure: the *2600* website circa 1998 features (very briefly) in the story, but I was plenty captivated before even knowing about that. It makes perfect sense that someone who was part of the hacker world would know about the "Free Kevin" movement - and that maybe that served as a bit of inspiration as to who they became and what they valued. We hear this all the time from actual human beings, but never before in a fictionalized work with such sincerity and lack of sensationalism. It's a small ingredient, there if you can appreciate it, that makes the storytelling a bit more solid. There are many other such moments, some captured in code, directory listings, and commands typed into a terminal. At one point, Elliot writes the name of a band on a CD that contains sensitive data instead. Was this an allusion to the Bradley Manning technique or just a method of disguise common amongst hackers? Either way, someone has done their homework.

The details of saving the world, starting a revolution, battling mental illness - or just what exactly comprises Evil Corp and the Dark Army - are best left to the viewer to try and figure out. Any theorizing here would reveal too much for those who have yet to dive in - and I suspect a fair number of intelligent people have hesitated to do this because of previous garbage we've all had to endure. (Now that the first season has aired, I recommend getting the DVD when it comes out. USA Network has an annoying habit of censoring some of the stronger language which winds up adversely affecting the stronger scenes. As a cable channel, they don't answer to FCC broadcast restrictions, so this is completely unnecessary and unwelcome. At the very least, they ought to air a late night version for those who can handle the occasional f-bomb.)

In reality, we're all just trying to get by and figure out what's right and wrong. And this is what Elliot Alderson struggles with throughout the story. He remains a true hacker regardless of the choices he makes and how he's manipulated. Sure, he breaks the rules a few times and invades the privacy of those he's interested in, as is the case with members of virtually every element of society. And as a hacker, he's very good at what he does. But it's all of us who make the world of lost privacy, powerful integrated/intelligent systems, and poor security a reality. This is what the media can never understand, that it's far more complex than the literal black and white they portray. It's about justice, vengeance, disclosure, a bit of fun, and ultimately finding yourself somewhere within it all. For that, *Mr. Robot* succeeds in bringing forth the most truly human portrayal of a hacker I've seen outside of real life itself. It's my hope that somebody will figure out a way for Chelsea Manning (and so many others) to see this while in prison for pursuing the same idealistic goals we celebrate here. It's more than a little therapeutic to have this sort of thing play out on the screen.

Now let's all hope they don't screw up Season Two with talking robots, cool graphics, or any scene that takes place in the Pentagon war room.

Cruising the Wideband Spectrum

by Agent T.W. Lee
Interzone Intelligence

Those new RTL-SDR USB stick receivers are a neat toy, but the author was interested in being able to look at a wider piece of the spectrum at a given time than what the RTL-SDR allows. The CIA and DOD have been using FHSS since the 1980s, so the author proceeded to look for old-school tech that could be used for wideband reception. Fortunately, such equipment can be readily found at hamfests and flea markets in this sector.

The old-school standbys are the wideband receivers and tuners made by Watkins-Johnson and CEI. No one seems interested in them anymore, and they can be found for under $100. Lesser-known brands such as Nems-Clarke, Grimm, and Astro are also around. Another piece of forgotten tech are the old analog NTSC TV service analyzers, especially those designed for CATV work. If one finds an old Wavetek SAM for under $50, they should snap it up. The CATV models have 3-300 MHz frequency coverage and can be used as a spectrum analyzer when hooked up to an inexpensive oscilloscope. The old SAMs can't be used to test the new digital TV systems, and many are gathering dust in old TV repair shops. Analog. Used to be that you could take your old click-tuner TV and tune between the channels. You'd also see static. Nowadays, you have preselected digital blue screen of death tuners. Think about the white spaces and in-between places. TVs used to go to Channel 83. They also used to go all the way down to 54 MHz. 54-88 MHz is bound to be useful now that the TV stations are gone. It at least will be interesting!

When I mean wideband, I mean from 100 kHz to 24 GHz. You never know where something interesting may be hiding in the spectrum! The author once saw Frequency Hopping Spread Spectrum in VHF high band. It was during a CIA/UFO/USAF experimental aircraft test. Took the author 20 years to find the equipment that did it at a New England hamfest. Preston bought up all the cool surplus WJ toys a while back, but now that he's retired and fixing tube amps for rich old hippies, you can find the stuff again, and it's pretty cheap for the moment.

Some of the newer stuff is pretty good too. The classic Radio Shack PRO-2006 is found for under $100 at many a hamfest because it does not do P25. You can always do an old-school discriminator tap and run any old police scanner into a PC soundboard and run DSD+ to decode P25, DMR, and TRBO. If you're smart, your PC will be running Linux. Yaesu, a few years back, came out with this receiver called the VR-5000 - one of the few ham-grade receivers with an IF output just like WJ and all the other pro gear, plus 100 kHz to 2.6 GHz frequency coverage! You can find them for sale cheap by scanner dweebs who weren't able to fully appreciate them. Hamfests, eBay, and QRZ are full of good tech waiting for you to take out and use.

Here is what the author does: He goes to

hamfests and looks around for likely prospects. His budget for an item is $200, maybe $300 if it's really nice. He does a quick function check. Scanners should be able to pick up the local 162 MHz NOAA weather radio stations. Shortwave receivers should be able to pick up WWV, some ham comms, and an international broadcaster like WBCQ with a few feet of wire stuck in the antenna connector. If so, then it passes the function check. Then knock about 30 percent off the asking price for a starting offer at the end of the hamfest. The seller will probably settle at about 15 to 20 percent off his asking price. What is a fair price? Look at completed *and* sold auctions on eBay. Average the prices you find and take another 30 to 40 percent off. That will roughly be a fair hamfest price. If the guy obviously has a good fair price on something, don't try to talk him down. Just pay for it and get out of there. Don't be an asshole!

The author prefers desktop receivers to portable units, as most of his radio research is done in a lab. You, on the other hand, may find portable units more towards your preference. Back in the days of his misspent youth, the author did a large amount of field work. The portable receivers of preference were a Radio Shack PRO-43 (yes, the diode was clipped for full 800 MHz coverage) and an Icom R10. Old Radio Shack scanners with 800 MHz were easy to mod for full coverage of the 800 MHz band by clipping a single diode. They pretty much killed that after 1994. The government does not make listening to certain frequencies illegal to "protect people's privacy." They are probably hiding something there. Now the RTL-SDR has full 800 MHz coverage, but it needs a PC to work. Find yourself a Radio Shack PRO-43, PRO-2005, or PRO-2006. Older Icom and AOR receivers are also good, but still command fairly high resale prices unless you are fortunate.

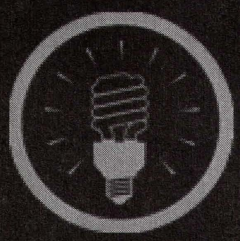
The deciding factor as to whether or not you should go portable or fixed/lab depends on what interesting things are going on in your county or neighboring ones. Go surf on over to `http://www.cufon.org/cufon/topufos.htm`. This is a list of the top 300 counties in the U.S. for UFO sightings. Since it is a known fact that the CIA and USAF have claimed responsibility for the vast majority of UFO-type sightings in the country, claiming they were experimental aircraft, this list right now is your best guide for determining if you should have a lab or a portable radio research setup. Keep in mind that aircraft communications can be heard 100-plus miles away due to their altitude. Land-based comms are 25 to 50 miles, maybe more, depending on the terrain. You can figure it out with that list! The author used to live deep in the heart of UFO territory, and heard/saw some amazing things. You just have to keep watching the skies and listening to the airwaves, but some of the best things he "heard" were not voice communications, if you get my drift!

So now that you have some gear, where do you start? A Google search of "spectrum use summary" (without the quotes) will show you a whole bunch of useful documents. Download them and use them as a guideline. Also, look for spectrum that appears to be underutilized, like TV broadcast "white space." Now that people can't tune between the channels like they used to, it has become a good place to hide in plain sight.

The best receivers, the author has found, are those that are tunable - as in tuning dial. The author started with 1960s and 1970s vintage multiband portable radios, and then upgraded to wideband surveillance receivers from CEI (Watkins-Johnson). Usually these units are wideband tuners with a 21.4 MHz IF output that you use with a demodulator or a shortwave receiver. The interceptor will discover lots more interesting emissions with this setup, especially when combined with a panoramic adapter/spectrum analyzer than he will with a police scanner on VHF/UHF+ frequency ranges.

OK, so you have some equipment and are ready to go. Start at the top end of your receiver's frequency range and tune down. Many improvised emitters are rich in harmonics and easier to find this way. Note every signal you find for later analysis. What the author does is start with an old-school analog receiver, log as much as he can, and then go back later with an RTL-SDR for a more in-depth analysis. He does this because he has discovered that the old-school analog gear works better for finding stuff than does the RTL-SDR. However, the RTL-SDR is better for signal analysis, especially when recording the characteristics of a signal over a period of time. The RTL-SDR has excellent Linux support, which is good because that is the OS you should be running.

EFFecting Digital Freedom



Let's Encrypt: Scaling HTTPS and TLS to the Whole Internet

by Jacob Hoffman-Andrews

If you were to design the Web from scratch today, each URL would start with HTTPS. Or rather, it wouldn't because you would build in encryption from the start, and it would be on by default. There would be no need to single out the more secure protocol as special.

We're stuck with the Internet we've got, however. Using HTTPS in place is simple, cheap, and effective. It's one of a tiny handful of encryption protocols that nearly everyone on the Internet uses every day, and most people are hardly even aware of it. But a majority of sites don't even offer HTTPS, let alone use it by default.

At the same time, the increasing affordability of mass interception and storage technology means that every action taken on a plaintext HTTP website is subject to spying. Worse, we've seen that browsers' default HTTP usage puts users at risk of hijacking to insert malware (QUANTUM), DDoS JavaScript (Great Cannon), tracking headers (X-UIDH), or advertisements (AT&T hotspots). Unencrypted should mean untrusted. But with the huge number of unencrypted sites out there, browsers can't start blocking HTTP content by default.

We are making progress, though. After Eric Butler's Firesheep extension viscerally demonstrated the ease of hijacking web sessions, large websites like Twitter and Facebook began implementing HTTPS by default. Google was already using HTTPS for GMail, but has since expanded their efforts to include most of their sites.

Major sites are able to dedicate time and resources to implementing HTTPS. But if we want to transition to an Internet where everything is encrypted, we want to make sure that transition doesn't increase the burden on individuals who want to speak on the Internet. It should always be possible to set up a server of your own, to express your own views to anyone who wants to listen, no matter how unpopular they are.

For a long time, HTTPS was inaccessible to most individuals. Purchasing the required certificate used to cost hundreds of dollars. With time, certificate prices have dropped dramatically, and now you can get a free certificate from StartSSL or WoSign. Still, though the monetary barriers are lower, the barriers of time and technical ability remain high. Experienced web administrators commonly take one to three hours to issue a single certificate. Less experienced people may fail completely. And the administrator must remember to renew each certificate every year, or their site will break: a surprisingly common occurrence, even for high-traffic web sites.

To secure the Internet, we need to make HTTPS ubiquitous. To make HTTPS ubiquitous, we need to make sure everyone can implement it, from the largest commercial site to the smallest forum, regardless of money or technical experience. This is why EFF and Mozilla, along with major sponsors Akamai, Cisco, IdenTrust, and Automattic, started Let's Encrypt.

Let's Encrypt will be a free, automated certificate authority, run by an independent non-profit, the Internet Security Research

Group. It will provide domain-validated (DV) certificates, which vouch that the person who controls a given hostname uses a certain public key for that hostname (the other major type of certificate, extended validation (EV), additionally vouches for the location and legal name of the entity behind a certificate, typically an organization. Since EV is not amenable to automation, it's not in scope for Let's Encrypt.).

There are three major components to the plan: a protocol, a certificate authority, and a client. ACME is a new protocol designed to cover the entire certificate life cycle, including domain name validation, issuance, renewal, and revocation. ACME meets the needs of Let's Encrypt, but our hope is that it will be more broadly adopted and become an Internet standard. To that end, there is an ACME working group at the Internet Engineering Task Force (IETF).

ACME is based on the recently standardized JSON Web Signature standard. After enrolling with the server, a client authenticates each of its requests by signing it with a JSON Web Key. To receive a certificate, the client must first prove that it controls each relevant hostname. The ACME protocol provides a challenge-response system that can be adapted to the policy of the CAs deploying it. For instance, a CA could request that the client provision a certain file at a well-known path on a web server that answers for that hostname, or require a code sent by email to an administrative address. Once the client has proved control of the hostname, it can submit a certificate request and receive an automated response.

To prove the usefulness of the ACME protocol, and (more importantly) to provide easy-to-use certificates for the Internet, ISRG is also creating a free CA. Let's Encrypt will have its own root certificate, which will be submitted to the various trust root programs for inclusion in browsers. However, to make sure the certificates it issues are immediately usable by the widest range of browsers, ISRG will also be getting its intermediate cross-signed by IdenTrust's root certificate. The Let's Encrypt certificate authority will operate using Boulder, a from-scratch implementation of the server side of the ACME protocol in Go.

The third and final component is the Let's Encrypt client. Besides speaking the ACME protocol, the Let's Encrypt client will perform two other important tasks: auto-configuring the new certificate in a local web server, and renewing the certificate periodically. Automated renewal is particularly important because expired certificates are one of the biggest causes of certificate warnings, and they are most commonly due to simple human error. Not only do expired certificates cause site downtime, they also train users to click through browser warnings. Auto-configuration is important because there are many common and time-consuming pitfalls in setting up HTTPS, such as forgetting to install an intermediate cert, or leaving the default, often insecure set of cipher suites. Not everyone will want to use Let's Encrypt's auto-configurator, though, and it will be possible to issue a certificate without installing it. And of course, ACME is an open protocol so anyone can write their own client. There are at least three third-party ACME clients already in the works.

Let's Encrypt is planning to launch to the general public on November 16, 2015. The code is available on GitHub, and all input is welcome, especially security analysis. If you find a vulnerability in Boulder or the Let's Encrypt client, please mail security@letsencrypt.org. For general questions, join us in the Let's Encrypt community support forums at `https://community.letsencrypt➥.org/`.

SUPPORT THE EFF!

Your donations make it possible to challenge the evil legislation and freedom restrictions we constantly face.

Details are at https://supporters.eff.org/donate.

The Dawn of the Crypto Age

by CANNON C.

Throughout all of the chapters of history, civilization struggles in a constant battle between liberty and tyranny, progression and corruption. For the world is plentiful in numerous points of its history of a populace oppressed by governments. Like a beast untamed or loosened, or a fire fueled and spread, it is the natural tendencies of governments to become corrupt and to perpetually expand and maintain power. This is not because government in itself is corrupt, but rather because mankind is corrupt through greed, in the pursuit of wealth and power at the expense of a nation while utilizing the powerful body of government as their tool. Government makes a handsome target of exploitation to the corrupt and enemies of liberty due to the centralization of power that governments wield and the position of the tool of government being in the high layer of power, known as the political realm.

Until now, the balance of power sat in the hands of governments who have gone rogue at the conduction of usurpers and tyrants and have been used to empower themselves while oppressing the populace and liberty, whether openly or covertly. However, in the modern age, in this dawn of the crypto revolution which follows the still advancing and parallel technological revolution, the balance of power in the world is shifting from that of governments and usurpers to the people.

Throughout history, humankind has been through various golden ages of enlightenment, and of technological advancements and progressions. It is this evolution in the advancement of humankind which has altered the foundation for which future technology and the direction of civilization is based. We have had the Age of Enlightenment, the scientific revolution, the Renaissance, the Industrial Revolution, and the technological/informational revolution, to name a few. And now, even when the latter is still young, we enter another age that parallels it: the dawn of the crypto revolution, which is based upon the infrastructure of the current technological/informational revolution.

The context of the word "revolution" in the case of this writing refers to that of sudden change in the world brought about by advancements in technologies and discoveries, while "crypto" or "cryptographic" is referring to the use of encryption (codes) paired with technology to create systems immune to espionage, control, and takedown by an enemy.

The newly emerging technology brought about by the crypto revolution is built on our current technological infrastructure. The advent of our current computerized cyber-infrastructure makes an easy way to build, host, and deploy decentralized protocols. It is also cyberspace that connects us all and breeds innovation through uncensored and decentralized communications such as the Internet, hence why the crypto revolution began shortly after the birth of the technological revolution. This new technology will secure itself and also secure society from the current flaws in our informational technology infrastructure which that same society has come to rely upon.

The crypto revolution will alter the shape of the workings of civilization in positive ways to advance us towards a more perfect civilization, just as the technological revolution altered the way we communicate, do business, interact, etc. And just as how the industrial revolution altered the way we travel, manufacture, and live, so too shall the crypto revolution shape our world. This time, this era in human progression will impact the workings of the economy, politics, banking, governments... all in a way that will make the workings of the pre-crypto age antiquated and perhaps even scoffed at by future generations.

Just as the crypto revolution is based on

the technological revolution which was based on the industrial revolution, so too shall some other future progressions be based on the crypto revolution. These future progressions as a result of the crypto revolution I foresee being comprised of political, economic, and social advancements.

Although progressions in the advancement of civilization are often beneficial to the human race, advancement is sometimes met with opposition by the existing power structure. This opposition by the minority who wield power over the rest is due to the threat this new technology/discovery presents to their power. Opposition can also often be due to lack of understanding of the new technology.

The future of technology I am describing can be referred to as decentralized cryptographic protocols - secure, open source, self regulating, decentralized, cryptographic protocols, to be more descriptive. For the new way will be a better way, a way void of the major flaws and imperfection of the former which have empowered the corrupt and created insecure systems causing results which have haunted our society. These newly emerging technologies will repair the security flaws which came about by having a society that became reliant upon informational technology. The root of many of the current security flaws in our world come from the exploitation of vulnerabilities that are a result of the lack of the following three items, which I refer to together as the triangle of security.

Integrity, Availability, and Confidentiality

Integrity. Through cryptographic proof. Protecting from unauthorized manipulation or forgery.

Availability. Through decentralization, keeping safe from attack by denial of service, or takeover by corruption and those security risks that are posed by centralization.

Confidentiality. Again, through cryptology. Keeping communications and information safe from unauthorized access.

The flaws caused by a lack of any part of this triangle of security can be mitigated with decentralized cryptographic protocols which address a solution for all three of these security needs.

A few examples of how the birth of cryptographic technologies will affect us in these three ways (not in any particular order but of equal importance):

Confidentiality: No longer can threats to the populace undermine the security of the world through informational-warfare/espionage with ease as civilization and informational infrastructure shall be secured with cryptology. No longer can governments, oppressors, and adversaries unjustly spy on a population with ease or target them for political gain, intimidation, persecution, or control. Cryptology will ensure confidentiality by preventing governments from spying on communications.

Availability: No longer will society be prone to attack by an adversary due to the weakness of centralization. When a society is reliant upon informational technology, as is the current case, that same society is vulnerable to a compromising of protocols and information that are centralized. For centralization introduces a higher risk of security due to a single point of failure. This is the case with both technology and government structures (an example being why governments are prone to corruption due to their centralization; even when governments are designed to be decentralized, they often becomes more centralized in power over time). Cryptology, in the form of decentralized cryptographic protocols, will ensure availability by preventing governments from taking down services, protocols, or information they do not like.

Integrity: No longer shall our civilization be vulnerable to spoofing, identity theft, fraud, or manipulation - whether that manipulation be of just a simple document, the voting results of public consensus, or other information (just to name a few examples). Through cryptographic proof, cryptography will ensure integrity and prevent tampering of data.

This is why information and technological dominance is a very valuable and sought after asset. In the technological/information age, unauthorized access to informational technology can compromise all security since everything runs on technology. These are the same security flaws which this newly emerging technology will help to protect us from.

Technology can be used against the people just as much as it can be used to empower

the people. This is why governments wish to suppress technological and, ultimately, human progression. For the future eliminates imperfection and corruption. We are now at the crossroads, in which technology used against the people is now progressing to the point that it will be used against corrupt governments and bring about a global balance of power. Governments also hate anything they cannot control. If governments cannot control something, they will attempt to destroy it.

Some of the changes, among many, which will be brought about by this new technology of decentralized cryptographic protocols will be decentralized markets immune to government control or takedown; distributed autonomous corporations and stock exchanges; self-enforcing smart contracts; secure and decentralized self-regulating financial systems known as crypto-currencies (such as Bitcoin); along with secure peer-to-peer escrow protocols resulting in anonymous and theft/confiscation-proof money, distributed crowd-funding platforms, and secure communications systems (such as Bitmessage or I2P-Bote); secure, anonymous, and fraud-proof identities; secure voting and consensus systems; distributed secure databases of information and records (such as Namecoin); legal document timestamping (known as "Proof of Existence"); secure property titles; secure wills and legal documents; secure distributed authentication systems; and distributed and anonymous reputation systems. Another result of crypto is meshnet networks immune to government control or surveillance that are known as darknets, which may eventually replace the current Internet infrastructure. The main structures of banks and governments may very well be replaced by secure, decentralized, self-regulating protocols which run on this technology. This is just to name a few things that will emerge or have started to emerge as a result of the crypto revolution.

Crypto technologies offer the ability to secure a population from the security flaws which cause identity theft, fraud, financial theft, corruption, manipulation, surveillance, and cyber attacks. Though this new technology protects society from such things which we suffer from today, it is also these things that governments and criminals use to control society and the populace. As a result, the security brought about by the newly emerging technology of decentralized cryptographic protocols threatens the ability of governments and criminals to continue their grip on a monopoly of control and power. Governments are often opposed to cryptology for this very reason. The suppression of cryptology is often done through "regulations" that are actually intended to cripple that technology, as well as outright bans on it, along with the targeting of its users. Another technique often deployed is use of the media to demonize cryptology through lies and fallacies - telling us that such technology is dangerous to our safety, when the truth instead is that the lack of cryptology leaves our liberties and our society insecure. Another fallacy often used to pass crippling regulations is that such technology *needs* regulation, which is a fallacy, for decentralized cryptographic protocols are already regulated by the principles of math which such protocols are built upon. These very rules of math which power these decentralized cryptographic protocols are perfect and incorruptible, unlike regulations done through government. Governments will try to suppress technology and human progression at the expense of the security of a nation, leaving us vulnerable to the security threats which currently plague our world - that is, if we allow ourselves to submit to tyranny by willingly complying.

There is a name for those who promote, develop, and support this crypto technology and who refuse to comply with the power structures' demands to abandon its progression. They are called the cypherpunks. They are the modern day architects, the visionaries of today, and the founders of tomorrow.

You can make a difference and help the crypto-age win. Join me. Join league with the cypherpunks to improve the world. At the least, learn about, support, and promote crypto technologies. If you are up to it, learn how to code so you can also contribute to these technologies. For we are now in the beginnings of a new era of advancement in civilization and the human race: the dawn of the crypto age.

Bitcoin Tip Address (to help support my writings): 1HcfM3dwy6zoT4kL2zWMD9qZRc➥sJdjiTST

Account Hack: Anyone Can Be a Victim

by lg0p89

Any account can be hacked. The attacker may use a tool for the password, a rainbow table, or other items to gain access. On a simpler level, the attacker may simply guess the password from social media clues. The motivation for this may be political (Sarah Palin's email account), for military intellectual property (a certain fighter plane), to gain access to a celebrity's email (Madonna and her stolen album), or a myriad of other reasons.

These breaches can be mundane or malicious. Recently, I was the victim of the latter with one of my PayPal accounts being compromised. I quite frankly have no idea how he would have acquired my passcode. The websites visited are not exciting or on the fringe. This account was only used twice in the distant past. Prior to this I had not had an issue.

Background

In March of 2015, I received an email from PayPal. This was a bit unusual due to this account not really being used. The only other emails that had been received had been when the account was opened and one or two other occurrences. Initially, I thought this was yet another phishing attempt and expedition. Everyone receives these from various sources from across the planet. After review of the header and the IP, it was determined this actually was from PayPal. The email stated that my account had been limited. With this being one of the PayPal accounts, I thought it was due to lack of use and did not think much of it. The next day, I received the same message from PayPal, which was strange. The same authentication method was used for the second email, which was also truly from PayPal.

Another week brought a new message indicating my address had changed to 25883 North Park Avenue; Unit A24509; Elkhart, Indiana. To ensure this was from PayPal, the email was authenticated. I have driven through Indiana, stopped occasionally, but do not know anyone living there. What also piqued my interest, other than the obvious, was that the unit number was unusual. It appeared this was not a suite or a unit from a multi-unit building due to the format.

Nerdy Sherlock Holmes

Anyone would be somewhat interested in what was going with their PayPal account, but the fact pattern made this more curious. At this point, I knew the PayPal account had been compromised and also knew something had to be done. If this person was willing to do this to me, anyone else would be fair game. This would be inherently unfair.

As much as Google is criticized, it is still a fantastic tool to gain information. The first step was to find out what was at the address. This would answer a few rudimentary questions first, which would limit the scope of my further investigation. If it were to be a residence, I would be able to get his/her cell phone numbers, email addresses, land line numbers (if applicable), where they work, their spouse's and children's names, and other creepy information. The address turned out to be the site of Viabox (`https://www.viabox.com/`). This entity provides a U.S. address and post office box. This allows whomever living wherever on the globe to receive mail that normally they would not be able to receive, as there are firms that don't ship outside of the U.S. I am sure all of their clients are completely law abiding and are not using the service to bypass or circumvent the applicable laws of the U.S. and respective states.

Viabox was contacted and informed of the circumstances on later that day. The representative at Viabox emailed back that they were sorry to hear about this and they work closely with "...several authorities to prevent fraudulent activities...." The response appeared to be a bit canned, as if this was not the first time they had received an email like mine. The fun aspect of this (for me) was I was able to secure the box owner's name (Firman Aulia) from Jakarta, Indonesia and his email address (firmanthole555@gmail.com). The company thankfully stated "We have sent a heads up on this with our Management and will cease shipping to this customer moving forward."

Summary

Technology is your friend. If someone elects to try and harm you, there are many ways to track them. Using basic social engineering, packet tracing, and other rudimentary tools, anyone is able to get the attacker's name, physical address, and where they are using their computer from.

The Stars Are Tomorrow

by LexIcon
lexicon@nc2600.org

Chapter One

Monsoon season had stared early, and the sounds of an overbuilt storm filled the terminal. It wasn't clear if Jenny saw Andy first, or it was the other way around. The lights had gone out for a few moments, causing both to look up from their laptops. They saw each other in momentary flashes of lightning, processing ghostly images of past life and present circumstances. The lights came back on and they were staring at each other across the VIP vaping lounge. Both looked away. Jenny looked back and thought she recognized the old backpack at his feet, and then she was the one who crossed over.

They had barely started talking when a gate agent's voice announced the cancellation of all flights out of New Business Luck City 77. Andy said he was going to go home, Jenny was going to stay in the terminal overnight and try to get out in the morning. She said she had given up her place in the city and was moving back home. Andy stayed and they talked a bit. Jenny said she had been traveling around Southeast Asia for a few months, and it wasn't what she had expected. She could never seem to visit places like Hashima Island or Kowloon Walled City. Andy said she had to come and stay with him. With a smile, he said, "my life is so cyberpunk now. You will love my place. I have a quick way out of here. You can rest up, get some good ramen, and fly out in the morning." She was apprehensive for a moment, running her fingers past her right ear, performing the absent minded time stalling action of brushing away hair, but it was no longer present with her tropics-friendly pixie cut. She looked down the concourse for a moment and suddenly changed her mind. "Yeah, let's go."

It took a couple minutes to walk all the way out with the crowd. When they got outside, the usual throng of beggars and unofficial porters was gone from the front door, driven away by the weather and disappointment at seeing a crowd bearing only carry-on luggage. There was a cab line with hundreds of people standing around, but only moments passed until Andy's housekeeper showed up in an old beat up green Mercedes with six miscellaneous antennas bristling across the roof. Jenny took note of yellowed copies of Gibson novels and new manga stuffed into the seatback pocket. Cyberpunk and scifi were what they had bonded over in high school, before he disappeared. So far he had only told her he had gone traveling; she was the one telling the stories.

The Mercedes exited the highway at the first opportunity, almost immediately after pulling on, then following a long road through an industrial-looking area before pulling up to an odd assortment of apparently residential buildings. The housekeeper said almost nothing the entire ride, and dropped them off at the end of an alleyway where the car could not proceed. Neglected laundry hung soaking in the rain from a line high above, sending down streams of water that they had to dodge around as Andy led Jenny a few meters into the alley and then up some green stone steps into a generic slum building. They rode upwards in an elevator that seemed surprisingly clean and safe considering the surroundings.

Andy's apartment was a penthouse that spanned two buildings and, contrary to Jenny's impression from the dilapidated exterior, it had been renovated into a mostly open floor-plan with modern fixtures and a cross of Eastern and Scandinavian aesthetics. There was a workbench near the kitchen, but really disassembled technology and half-finished projects were everywhere. This was a hackerspace.

After drying off a bit, the two settled onto a western-style couch, and Jenny pressed again for an answer as to why Andy had disappeared all those years ago.

"Would you believe I won the lottery?" Jenny just smiled and raised an eyebrow skeptically. "Do you remember how my dad was always throwing away my comic books and anything that wasn't for school? So, it was my 18th birthday, and you and some other people had given me some really great stuff, and my dad came into my room and ripped it all up, even snapped two CDs in half. As he was tearing out the pages of *The Stars My*

Destination, he kept screaming 'the stars are tomorrow, the stars are tomorrow, the stars are tomorrow.' It was a major blowup. I made the mistake of screaming back at him, and he hit me hard. I snuck out of the house that night and hitchhiked to see my godfather, Lewis Grand, who was my mom's mentor when she was working in Chicago. He and my dad hated each other. Well, my dad hated Lewis, anyway. When I got there, he was so happy to see me. I didn't know if he would even remember who I was. He made me dinner, and it was my mom's lemon chicken recipe... rather, it was his recipe that she used. We talked half the night, and I could just feel this weight lifting. I hadn't trusted anyone in a long time, but I immediately trusted Lewis."

The housekeeper came in the door. "Fung, when you're dried off, would you make us some tea and a snack, please?" She nodded silently and trudged off toward the back of the apartment. "Who is that?" asked Jenny. "She's my housekeeper. Her niece used to work for me, but she was in an accident a few weeks ago, so Fung came to live with me." Jenny got a weird vibe from her, but wasn't sure why, so she prompted Andy to keep telling his story.

"The morning after I got to Lewis's house, there was this envelope on the coffee table with my name on it, and a birthday card inside that just said 'cash me.' Taped inside the card was a $20 bill and a lottery ticket. Lewis wasn't in the house, so I walked down the street to a convenience store on the corner and got a fried egg and mayo sandwich, and asked the guy to check the ticket... six million dollars. I didn't even have a bank account. It was insane. When I got back to the house, Lewis was there, and he was playing it all cool. I don't know what he did, but I don't think I won the lottery by random chance. He asked me what I wanted to do most, and I said I wanted to go see all those places in the books. So, he helped me set up a bank account and pick my first destination, and then I was off. Traveling the world, looking for Mr. Lee's Greater Hong Kong, or Morpheus, or whatever the hell else was out there."

Andy went on, with Jenny starting to ask a lot of questions. He told her about the year in Shanghai, the year in Tianjin, living with the Tungusic and Mongols, and how he had met so many hackers and tinkerers in the Philippines. He didn't just burn the lottery cash, he had started making business deals, trading his knowledge of tech and cultures for shares in dozens of companies. Finally, he got a bit self conscious and realized he had been talking for hours. He wanted to know what brought Jenny to the city, but she dodged most of his questions. She kept getting up and looking out the window. Finally, Andy got up and went to see what she was looking at.

Down on the street, at the corner near the shuttered solenoid factory, just at the edge of the streetlight, a figure. The rain was temporarily abated, still falling but not nearly as hard. This person was just standing there in a wide brimmed hat and a trenchcoat - conspicuously western. "Who is that?" asked Andy. "Nobody. It's nobody." Jenny walked away from the window. "How do you know it's nobody? Who is that?" Jenny looked pained and rubbed the back of her arm.

It was at that moment they heard the hammers being pulled back on handguns from across the room. Three men in suits with tattooed faces had somehow entered the apartment unnoticed, and two were approaching with guns drawn. Andy put his hands up and stood between them and Jenny, while she stuck her hands deep in her pockets and backed up against the window. They didn't want Andy, they wanted Jenny.

Less than a minute and a half later, Andy and Jenny were running down the slick wet alleyways of the oddly assembled apartment block, with the housekeeper and a trenchcoated American whom Jenny had introduced as Monticello but addressed as Monty. Andy's lip was busted open and he winced a bit every few steps. Monticello held a handkerchief against a gunshot wound in his left shoulder but otherwise looked more or less unstoppable. One of those unreal action movie types who gets character from taking bullets and shovels to the head. They ran through a shopping arcade with huge spreads of vegetables and big baskets and cages full of small animals destined for stews, then turned and were in a red light district, then Andy led them through a brightly-lit cooking store that cut through the block, and down another alley into a basement with a strobing LED sign over the door that was so bright it almost hid the entrance.

This was Mandibles, a 187-station cybercafe, populated by gamers and travelers, businessmen and hustlers, kids and caff junkies... a dimly lit sea of screens and task chairs in row after row of cubicles and desks and zombies with headphones. No one paid much notice

to the four soaking wet figures rushing down a sparsely populated row of older machines and practically crashing into the back room where they found the manager, Lim Ling, poking at a tray of takeout pork dumplings.

Andy was upset that no one was at the front desk. This was his business, and Lim was supposed to be on duty. Lim solemnly nodded to Andy, but couldn't stop staring at Monticello's painfully obvious gunshot wound. Andy sent Lim back to the front desk and ordered no disturbances. There was a first aid kit in the office, and Jenny showed surprisingly efficient medical skills, carefully extracting the bullet and suturing the wound.

"Where did you learn to do that?" asked Andy with a raised eyebrow. Jenny hesitated as Monticello glared at her, but after a moment she shook off his apprehension and her own, and started to explain. "Basic training. We're agents of The Nodes. I was headed back stateside when I ran into you at the airport. I was carrying something very important. Remember all those diplomatic cables that WikiLeaks dropped on the web a while back? Think bigger. So, it was supposed to be a silent operation, but those gangsters showed up right when you asked me to hang out."

The Nodes: National Observation and Defense of Electronic Systems and, as Jenny said, "we're a kind of cyberpunk CIA, an intelligence agency not answerable to DHS, a quasi-public enterprise. Corporate donors fund our operations to keep an eye on the electrons. We operate where hackers operate, where financial transactions happen, and keep hubrisine foreign corporations honest by reading their mail." Andy wasn't sure if she was joking or trying to scam him. The Nodes was popularly exaggerated, a running joke in the ex-pat tech community - like every cell phone, every ATM, every $12 generic electric beard trimmer on the planet was a piece of their surveillance network.

The gangsters would find them soon. All licensed businesses in the city had to point a surveillance camera at people walking in the front door, and all the feeds went back to a police surveillance system. At Mandibles, the system was conveniently transmitting static, and Andy was literally sitting on a pile of government notices about fines for noncompliance, but they had run past two dozen other businesses that weren't expressing a state of willful disobedience. The police weren't the problem exactly. It was the tech-savvy criminal gangs who regularly tapped into the system and its facial recognition database. Even if the gangsters chasing them didn't have regular access, they surely could get a favor in a matter of minutes, and with frightening precision narrow down accurate last known whereabouts. As soon as the group had passed through the cooking store, they were undoubtedly on the police radar, and in turn the gang's. Everyone knew this, but Andy had a plan.

"Bad Pandas," said Monty. He was looking out through the dark glass at the front door, where Lim was face down in his dumplings at the front counter, and the gangsters were already inside Mandibles, moving row to row roughing up the customers. Monticello recognized one as a leader of the notorious crime ring, Shulanqui Bad Pandas, who specialized in data ransoming. Jenny wondered aloud, "That was too fast. Monty, how did they know?" That was also the moment that the old housekeeper, Fung, inexplicably turned on the overhead lights in the back room, canceling the effect of the two-way mirror, and drawing the attention of the gangsters like velociraptors to a fallen spoon.

The group fled out a back door, deeper into the building and up to the roof. High above the dense concrete and steel blocks of the neighborhood, the rain had subsided, and blinding sideways electronic billboard light punched through a haze across the slick concrete flattops and corrugated aluminum lean-tos that framed the garden and birdcage penthouses, creating a mix of simple and complex deep shadows from the kaleidoscopic matrix of architecturally slapdash rooftop geometries. Even being chased by gunmen, Jenny looked around in a moment of wonder. After navigating over a dozen puzzle box parapets, and Monty taking down a perhaps innocent camera drone with his sidearm, they descended again into yet another stark concrete stairwell.

Now they were in a long hallway, multiple buildings connected with covered bridges. Andy seemed sure of where he was going. There was music ahead, and then all around them, but Jenny couldn't tell where it was coming from. Andy stopped in front of a large air vent and knocked on the opposite wall. A panel slid open and a fierce scowl eyed them closely. The vent popped back and slid open, and Andy led the group into the wall.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 9-10
GrrCON
DeVos Place
Grand Rapids, Michigan
www.grrcon.org

October 16-18
Maker Faire Rome
La Sapienza, University of Rome
Rome, Italy
www.makerfairerome.eu

October 21-25
ToorCon 17
San Diego Westin Emerald Plaza
San Diego, California
sandiego.toorcon.net

October 23-25
Pumpcon 2015
Khyber Upstairs (56 S 2nd Street)
Philadelphia, Pennsylvania
www.pumpcon.org

October 24-25
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

November 6-7
PhreakNIC 19
Clarion Inn Murfreesboro
Nashville, Tennessee
phreaknic.info

December 10-11
Kiwicon 9
Wellington, New Zealand
www.kiwicon.org

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

January 15-17
ShmooCon
Washington Hilton Hotel
Washington DC
www.shmoocon.org

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

PROTECT YOUR PRIVACY ONLINE. FoxyProxy sells VPN and proxy services. Why choose us? We've been around since 2006 and have always been privately owned, independently operated. We don't have any shareholders or venture capitalists to satisfy by compromising your privacy. No advertising. No logging. No spamming or marketing emails. We don't sell your email address and other information. WE ARE HUGE OPEN-SOURCE CONTRIBUTORS. All accounts come with both VPN AND proxy service. Choose from 60 different countries. Use coupon code "2600-hope" for 10% off any purchase. getfoxyproxy.com

PRIVACYSCAN seeks & destroys privacy threats on the Mac wiping your tracks on where you surf and what you do on your computer. Learn more at http://privacyscan.securemac.com/

HACKER CLOTHING & GEAR - HackerStickers.com has a growing selection of hacker, gamer, geek, and security advocate clothing, hardware, caffeine, stickers, lock picks, patches, pins, etc. *2600* readers get a free sticker with any order. Add a sticker to cart and enter code "FREESTICK" at checkout at HackerStickers.com.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in the background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. Handles Bluetooth Classic and Bluetooth LE (on LE-equipped Android devices). This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download at http://tinyurl.com/btscan.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com. We are now working to supply stores nationwide - full details at club-mate.us.

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com.

ET PHONE HOME FOB: Subminiature, tiny (7/10 ounce), programmable/reprogrammable touch-tone multi-frequency (DTMF) dialer with key ring/clip which can store up to 15 touch-tone digits and, at the push of the "HOME" button (when held next to a telephone receiver), will output the preprogrammed telephone number which can be heard at the same time from the unit's internal speaker. Ideal for E.T.'s, children, Alzheimer victims, significant others, hackers, and computer wizards. It can be given to that guy or gal you might meet at a party, supermarket, or social gathering when you want him/her to be able to call your "unlisted" local or long distance telephone number, but want to keep the actual telephone number confidential and undisclosed. Only you have the special programming tool to change the stored number. Limited quantity available. Money order only: $28.95. Order two or more, then only $24.95 each. Add $4 S/H per order. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas, Box 410802, Crc, Missouri 63141.

OPEN POWER: *Electoral Reform Act of 2015 - Open Source Activist Tool Kit* by HOPE speaker Robert Steele available on the Kindle and at amazon.com

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we strive to carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

Announcements

HAVE YOU SEEN THE NEW *2600* STORE? We've finally made the jump into the 21st century with a store that has more features, hacker stuff, and endless possibilities than ever before. We now accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have more digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

Wanted

I NEED A LAWYER for ineffective assistance of counsel. I'm Jesse McGraw (3:09-CR-210-B), and seeking relief for damages against prior attorney for breach of fiduciary duty, attorney-client confidentiality, and effective abandonment of my 2255 Appeal. He tried to inform against me, my 2255 was never filed, and there's critical (Brady) evidence missing from my case file. (I'm on a botnet/hacking case.) freejesselegalteam@hush.ai, freejesselegal.wix.com/freejesse

PHREAKNIC 19 CALL FOR SPEAKERS. PhreakNIC is a small (~200 attendees) technology conference run by the Nashville *2600* Nonprofit, with an eye towards subjects interesting to the *2600* crowd. This is our 19th year, and PhreakNIC 19 will take place November 6-7, 2015. A number of speakers who have gotten their feet wet at PhreakNIC or similar small conferences have then gone on to speak at larger conferences such as Def Con and Black Hat. To see lists of past speakers, check http://phreaknic.info/history.html. We are looking for all types of talks and workshops, including but not limited to 0-days, hardware hacking, darkweb/darknet, lockpicking, cryptocurrency, pen testing, anything bleeding edge or even historical if it

might be of interest to tech/security geeks. If you'd like to speak, please send a description of your proposed talk to speakers@nashville2600.org.

Services

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

LISTEN TO THE GR3YNOISE PODCAST. The podcast formerly known as the SYNACK Pack is now GR3YNOISE! There are many security minded podcasts out there, and we're one of them. We are here for the newbies and veterans alike! The GR3YNOISE Pack podcast discusses general news as well as technology specific issues, all from a hacker perspective. Recorded at the SYNShop Hackerspace in downtown Las Vegas, NV. Have a listen and we LOVE feedback! http://gr3ynoise.com or http://greynoi.se.

DATA RAIN SOLUTIONS is a budding Colorado IT startup specializing in reliable and affordable remote tech support in advanced malware removal, PC optimization, diagnostics, and more. *2600* subscribers get 10% off their first order, as-need basis, or 1 year sub. Contact us: shanaroneasomi@yahoo.com. Visit us: http://shanaroneasomi.wix.com/datarain. Join the team! (Hackers welcome)

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMINAL CRIMES? Stand up for your rights! Be calm, respectful, and clear: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to speak to a lawyer." Remember basic game theory and the Prisoner's Dilemma: if nobody talks, then everybody walks. In the event of unwanted police contact, it would be advisable to consult with a lawyer experienced in defending human beings facing computer-related accusations in California and federal courts. I am an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of hacking, cracking, misappropriation of trade secrets, and other cybercrimes. I am a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and I am willing to contribute pro bono representation for whistleblowers and accused hackers acting without malice. Past clients include Kevin Mitnick (million-dollar-bail case in California Superior Court dismissed), Robert Lyttle of The Deceptive Duo (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure), and Vincent Kershaw, reported member of Anonymous indicted for his alleged participation in a DDOS action against PayPal. Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note I also specialize in Constitutional and criminal defense of cannabis cases as well as legal compliance with a complex maze of marijuana-related laws and regulations. Please contact Omar Figueroa at (415) 489-0420 or (707) 829-0215, at omar@stanfordalumni.org, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

INTELLIGENT HACKERS UNIX SHELL: Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data from many sources, including computers, external media, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei's digital forensic examiners all hold prestigious forensic certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and hundreds of articles on digital forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at (703) 359-0700 or email us at sensei@senseient.com.

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and web sites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) offers free DNS hosting and WHOIS privacy for $3.50 with all domains registered or transferred in!

Personal

STORMBRINGER IS STILL ALIVE AND WELL in Club Fed. 15 yrs thus far, 4½ to go. Looking for correspondence to pass the time. A geekette would be nice, but anyone can also write. Looking also for white papers in infosec, networking, etc., so I can hit the ground running upon release. Henry French, where R U? www.freestormbringer.com W.K. Smith, 44684-083, P.O. Box 999, Butner, NC 27509-0999.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com.

Deadline for Winter issue: 11/21/15.

Have you seen the brand new *2600* store? We have moved over to Shopify after 16 years with Yahoo. The nearly unanimous opinion so far is that this move was long overdue. Not only do we have a completely different look, but we have a lot more flexibility along with options that will benefit you and help us expand and innovate.

We have all kinds of items of hacker history as well as brand new things we believe will intrigue and fascinate. In addition:

- We now acccept Bitcoin.
- We now accept Google Wallet.
- We continue to accept PayPal and all major credit cards.
- We have far more flexibility in the products we can offer. This means more digital offerings as we can store massive files on this new service.
- More accurate shipping rates, rather than the wild guessing that was necessary on our old store.
- More shipping options.
- Downloadable HOPE videos in MP4 format with no DRM in full DVD quality.
- Overall lower prices.
- Complete SSL encryption, security, and privacy for everything you type and view.

Coming soon:

- Gift cards.
- The ability to renew online (without your subscription info being on the net).
- Optional accounts for frequent visitors.
- Probably a lot more we haven't figured out yet.

COME VISIT US AT

STORE.2600.COM

"There is very little that you will encounter in life that has not been infused with bullshit." - Jon Stewart, 2015

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Bruce Haack, Happy Kyne and the Mirthmakers, Mindless Self Indulgence

Shout Outs: Ahab, Bear, Bruno, Capella, Chevy, Cozzy, Daniel, Dru, Goblin, Kraken, Lasher, Maude, Maya, Medusa, Moe, Myra, Nicky, Nutok, Phanty, Pumpkin, Rattles, Reculse, Red, Rocket, Roo, Shrek, Simba, Siren, Spike, Stella, Storm, Stubby, Wayne, Zeus

Thank You: Jonathan Liebowitz

R.I.P. Don Joyce, Owen, Bill Acker

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 (ISSN 0749-3851, USPS # 003-176); Autumn 2015, Volume 32 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2015 are $27 per year or $6.95 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2015; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bodegon Bellagamba, Carlos Calvo 614, San Telmo. In the back tables passing bathrooms.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Ourimbah RSL (in the TAB area), 6/22 Pacific Hwy. 6 pm
Melbourne: Oxford Scholar Hotel, 427 Swanston St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver (Surrey): Central City Shopping Centre food court by Orange Julius.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.
Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm
Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm
Paris: Cafe Monde et Medias, Place de la Republique. 6 pm
Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm
Rouen: Place de la Cathedrale, benches to the right. 8 pm
Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the payphones beside the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm
***Safed:** Courtyard of Ashkenazi Ari.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

Scotland

Glasgow: near the Cenotaph in George Square. 6 pm

Wales

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Arizona

Phoenix: HeatSync Labs, 140 W Main St. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Anaheim (Fullerton): The Night Owl, 200 N Harbor Blvd. 7 pm
Chico: Starbucks, 246 Broadway St. 6 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar.
Monterey: East Village Coffee Lounge. 5:30 pm
Sacramento: Hacker Lab, 1715 I St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Loveland: Starbucks at Centerra (next to Bonefish Grill). 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

Delaware

Newark: Barnes and Nobles cafe area, Christiana Mall.

District of Columbia

Arlington: Rock Bottom at Ballston Commons Mall. 7 pm

Florida

Fort Lauderdale: Undergrounds Coffeehaus, 3020 N Federal Hwy. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: O'Brothers Irish Pub, 1521 Margaret St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Titusville: Krystal Hamburgers, 2914 S Washington Ave (US-1).

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm
Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: Tomlinson Tap Room in City Market, 222 E Market St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm
Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Las Vegas: SYN Shop, 117 N 4th St. 7 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Morristown: Panera Bread, 66 Morris St. 7 pm
Somerville: Dragonfly Cafe, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm
New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Cup A Joe, 3100 Hillsborough St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 5:30 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm
Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm
Nashville (Franklin): CoolSprings Galleria food court, 1800 Galleria Blvd. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
Houston: Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia

Arlington: (see District of Columbia)
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm
Spokane: The Service Station, 9315 N Nevada (North Spokane).
Tacoma: Tacoma Mall food court. 6 pm

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Spanish Speaking Payphones

Mexico. Found in Palomas in the state of Chihuahua, this phone clearly has its share of traffic and is in pretty good shape.

Photo by Fred Atkinson

Mexico. This colorful wi-fi phone was spotted in Mérida in the state of Yucatán and doesn't appear at all worse for wear.

Photo by carlos duarte

Cuba. An ETECSA (Cuban government's telecommunications enterprise) payphone seen in Havana. It doesn't appear to take coins.

Photo by Lee317

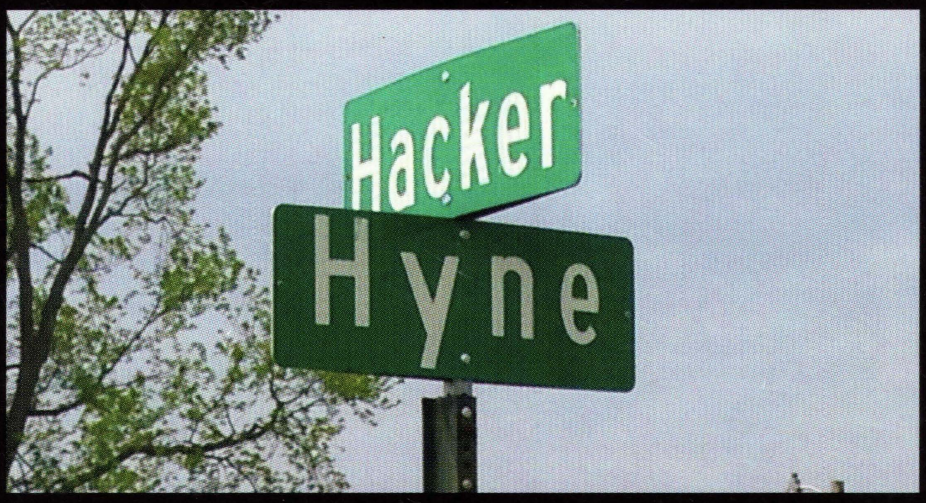
Spain. Another pristine payphone model found in Rota in the southern region of Andalusia.

Photo by Fred Atkinson

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

Now this is the kind of joint we all should stay in at least once. Hell, maybe we could even have a convention here! The person who submitted this gave us absolutely no details on its location (thanks for that), but since they sent it from their phone, with a little detective work we figured out it was in Chicago. We can feel this place calling to us. *TripAdvisor* raves "WORST hotel ever" and "Horrible and Disgusting," but we believe those are just clever ploys to try and keep us away.



Seen in Brighton, Michigan by **Gary Rimar**, this intersection is particularly great because it leaves out the word "Road" on each sign, making it possible for all sorts of jokes and allusions to work. We'll leave that as an exercise for the reader.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to *2600* Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.